جرائم الإنترنت والحاسب الآلى

ووسائل مكافحتها

منير محمد الجنبيهى

المحامى

عضو إتحاد المحامين العرب

ممدوح محمد الجنبيهى

المحامى

عضو إتحاد المحامين العرب

2004

الناشر

دار الفكر الجامعى

٣٠ ش سوتير الازاريطة ـ الاسكندرية

ت : ٤٨٤٣١٣٢

جرائم الإنترنت والحاسب الآلى

ووسائل مكافحتها

منير محمد الجنبيهى

المحامى

عضو إتحاد المحامين العرب

ممدوح محمد الجنبيهى

المحامى

عضو إتحاد المحامين العرب

2004

الناشر

دار الفكر الجامعى

٣٠ ش سوتير الازاريطة ـ الاسكندرية

ت : ٤٨٤٣١٣٢

المقدمة

سبق وان أصدرنا العديد من المؤلفات في مجال القانون التجاري و العقود التجارية إلا انه و مع التقدم التكنولوجي المتوالي و الذي نعيشه منذ عقد مضى تطورت أساليب التجارة و أصبحنا نجد الآن عمليات تجارية تتم عبر شبكة الإنترنت فيما يعرف بالتجارة الإلكترونية و ما يشمل ذلك من عقود إلكترونية و توقيع إلكتروني و مستندات إلكترونية و ما إلى ذلك من أشياء أصبحت كلها الآن إلكترونية بفضل التقدم التكنولوجي في كافة المجالات •

و عليه قد سبق و أن أصدرنا مؤلف عن التوقيع الإلكتروني و حجيته في الإثبات و الآن نقدم هذا المؤلف عن أخطار شبكة الإنترنت المتمثلة في جرائم الإنترنت و وسائل مكافحتها •

آملين أن يجد كافة مستخدمي شبكة الإنترنت و كذلك العاملين بالقانون في مؤلفنا هذا خير المعين و نعم المساعد الأمين

المؤلفان

منير محمد الجنبيهي

ممدوح محمد الجنبيهي

المحاميان

بالاستئناف العالي و مجلس الدولة

عضوا اتحاد المحامين العرب – عضوا اتحاد المحامين الأفروآسيوي

مستشاران قانونيان بالأمانة العامة للحزب الوطني الديمقراطي بالإسكندرية

مكتب / ٢١ شارع السمان – مصطفى كامل – الإسكندرية

تليفون مكتب / ٥٤٤٤٣٦٩ / ٠٣– محمول / ٠١٢٢٦٧٩٠١٣ / ٠١٢٣٨٦٤٩٧٩

الفصل الأول

ماهية الإنترنت

WHAT ABOUT THE INTERNET

يعتبر الإنترنت - الذي بدأ العمل بتاريخ ٢ / ١ / ١٩٦٩ عندما كونت وزارة الدفاع الأمريكية فريقا بحثيا من العلماء بمشروع بحثي كان موضوعه هو تشبيك الحاسبات - هو ثمرة التقدم العلمي العالمي في مجال الاتصالات و تبادل المعلومات و تعتبر شبكة الإنترنت INTERNET هي الشبكة الرئيسية التي تجتمع تحتها كافة الشبكات الأخرى أيا كان نوعها أو الغاية منها أما شبكة الإنترنت فإنها تتكون من عدد كبير جدا من الشبكات المترابطة و المتناثرة في كافة أنحاء العالم و من المعروف أن البروتوكول الذي يحكم كافة تلك الشبكات هو بروتوكول واحد هو البروتوكول المسمى (بروتوكول تراسل الإنترنت - TCP / IP) •

وكانت وزارة الدفاع الأمريكية قد كونت فريقا من العلماء للقيام بمشروع بحثي حول إنشاء شبكات تربط فيما بين أجهزة الحاسبات الإلكترونية COMPUTER وكان أساس البحث في هذا المشروع البحثي بجانب إنشاء الشبكات هو تجزئة الرسالة المراد إرسالها إلى موقع معين في الشبكة و من ثم يتم نقل كل جزء من تلك الأجزاء بسلك طريق مختلف عن الطريق الذي تسلكه الأجزاء الأخرى من الرسالة MESSAGE حتى تصل تلك الأجزاء جميعا ثم تتجمع ثانيا فتتكون الرسالة مرة أخرى كما كانت مرسلة •

وكانت أهمية أجراء تلك الأبحاث لوزارة الدفاع الأمريكية في غاية الأهمية حيث كان ذلك في آتون الحرب التي أطلق عليها مصطلح (الحرب الباردة) والتي كانت قائمة على اشدها فيما بين الاتحاد السوفيتي (والذي تفكك إلى جمهوريات مستقلة الآن) و الولايات المتحدة الأمريكية •

فقــي حالـــة مـــا إذا تــم اعتراض أي من أجزاء تلك الرسالة و دمرها الاتحاد السـوفيتي فأن بقية أجزاء الرسالة تكمل طريقها إلى منطقة الوصول و من تلك الأجـزاء التـــي استكملت طريقها يتم جمعها وبالتالي يمكن فهم فحواها و العمل بمـا فيها من تعليمات دون أن يكون للاعتراضات و عمليات التجسس السوفيتي أي اثر يذكر على تلك الرسائل .

ومــن هنا كانت أهمية هذا المشروع البحثي و أهمية التجارب التي كانت تجرى من خلاله إلى وزارة الدفاع الأمريكية .

ثــم تطور المشروع بعد ذلك إلى الاستعمال السلمي بجانب الاستعمال العسكري حيث انقسم عام ١٩٨٣ إلى شبكتين احتفظــت الشبكة الأولى باسمها الأساسي (ARPANE) و بالغــرض الأساسي الذي نشأت من اجلــه وهو خدمة جهاز المخابــرات المركزية الأمريكية و يرمز إليها بــ (C I A) و سميت الشبكة الأخــرى باسم (MAIL NET) و تلك الشبكة تم تخصيصها للاستخدامات المدنيـــة التي خصصـــت للاستخدام السلمي المدني و من ثـــم ظهــر اسم (ENTER NET) وفــي عــام ١٩٨٦ م أمكــن ربـــط خمـــس مراكــز للكومبـيوترات العملاقـــة و أطلــق علــيها اســـم (NSF NET) و التي أصبحـــت فيما بعد العمــود الفقري و الأساسي لنمو و ازدهار شبكة الإنترنت في الولايات المتحدة الأمريكية ثم دول العالم اجمع بعد ذلـــك .

من يملك الإنترنت

THE OWNER OF THE INTERNET

في البداية كانت الحكومة الأمريكية هي المالك لشبكة الإنترنت ثم انتقلت الملكية إلى المؤسسة القومية للعلوم (مؤسسة أمريكية) ألا انه في الوقت الحاضر لا

يمكــن القــول أن هناك مالك لشبكة الإنترنت فليس هناك مالك و إنما هناك ما يســمى بمجــتمع الإنترنــت و ليس هذا فقط و إنما أيضا التمويل فبعد أن كان الــتمويل حكومــيا اصبح التمويل يأتي من القطاع الخاص ومن هنا اصبح هناك العديــد و العديــد مــن الشبكات الإقليمية ذات الغرض التجاري و التي تعرض الاستفادة من خدماتها بمقابل مالي ٠

توسع الشبكة

EXPANSION IN THE INTERNET

فــي عام ١٩٨٥ م كان هناك اقل من ألفي حاسب إلى مرتبط بالشبكة وفى عام ١٩٩٥ م وصــل العدد إلى خمسة ملايين حاسب إلى مرتبط بالشبكة و في عام ١٩٩٧ م وصل العدد إلى ستة ملايين حاسب وهى تستخدم حوالي ثلاثمائة ألف (SERVER) متــناثرة فــي كافــة أرجاء العالم وبالنسبة لعدد المستخدمين فيمكــن القــول انه ينضم ستة و أربعين مستخدما جديدا للشبكة كل دقيقة على مستوى العالم ٠

و فــي اســتطلاع للــرأي أجــرته شــبكة (N U A) الأمريكية قــدر عــدد مستخدمي شبكة الإنترنت USERS OF THE INTERNET عالميا في عــام ١٩٨٨ م بحوالــي مائــة و أربعــة و ثلاثين مليون مستخدم و تصدرت الولايات المتحدة الأمريكية و كندا الصدارة من حيث عدد المستخدمين الذي بلغ ســبعون ملــيون مستخدم (N U A . 6 / 1998) وفــي تقريــر أجرته و نشــرته أيضــا شــبكة (N U A) الأمريكيــة و صــدر بتاريخ ٢٦ / ١٠ / ٢٠٠٠ قــدر أن عــدد المستخدمين للشبكــة في عام ٢٠٠٥ سيكــون حوالي مائتان و خمسة و أربعــون مليون مستخدم كما أن هــــذا التقرير قــد قــرر

أيضـا أن اغلـب تلـك الزيادة من مستخدمي الإنترنت ستكـون من خارج الولايات المتحدة الأمريكية (N U A . 10 / 2000) ٠

علـى أن عمليات تطوير شبكة الإنترنت لم تتوقف DEVELOPING OF INTERNET DID NOT STOPOVER قط فقد أشار الرئيس السابق للولايات المتحدة الأمريكية (بيل كلينتون) إلى مشروع مستقبلي لتطوير شبكة الإنترنـت أطلق عليه اسم (الإنترنت ٢) (ENTER NET 2) أو الجيل الثانـي مـن الإنترنت فقال (لابد من أن نبني الجيل الثاني من شبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة و مختبراتنا القومية للتواصل بسرعة تزيد ألف مرة عن سرعات اليوم و ذلك لتطوير كل من العلاجات الطبية الحديثة و مصادر الطاقة الجديدة و أساليب العمل الجماعي) ٠

وكانـت شـركة (STAR BAND) قـد أجرت تجربة في شمال الولايات المـتحدة الأمريكية عن مشروع لشبكة إنترنت بواسطة الأقمار الصناعية بلغت سـرعته حوالـي خمسـمائة - كـيلو / بايت - في الثانية الواحدة من شبكة الإنترنـت إلـى الحاسـب الآلي COMPUTER وهو ما يعد قفزة هائلة في سرعة البث ٠

خدمات شبكة الإنترنت

SERVICES OF THE INTERNET

١ - البريد الإلكتروني (E - MAIL)

لإرسال و استقبال الرسائل بسرعة كبيرة جدا

٢ - القوائم البريدية

إنشاء و تحديث قوائم العناوين البريدية الخاصة بمجموعات من الأشخاص ٠

٣ - خدمة المجموعة الأخبارية

وهـــى تشـــبه خدمـــة القوائم البريدية ألا إنها تختلف في أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها ٠

٤ - خدمة الاستعلام الشخصي

حيث يمكن من خلال هذه الخدمة الاستعلام عن العنوان البريدي لآي شخص أو جهة تستخدم الإنترنت و المسجلين لديها ٠

٥ - خدمة المحادثات الشخصية

حيث يمكن التحدث مع طرف آخر صوتا و صورة و كتابة

٦ - خدمة الدردشة الجماعية (CHATING)

تشـــبه الخدمـــة الســـابقة ألا اتـــه وفى الغالب يمكن لأي شخص أن يدخل في المحادثة أو يستمع إليها دون اختيار الآخرين

٧ - خدمة نقل الملفات

(F T P) لنقل الملفات من حاسب آلي إلى حاسب إلى آخر وهى اختصار كلمة (FILE TRANSFER PROTOCOL)

٨ - خدمة الأرشيف الإلكتروني

(ARCHIVE) تمكـــن مـــن البحـــث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم ٠

٩ - خدمة شبكة الاستعلامات الشاملة

(GOPHER) تفيد في خدمات كثيرة كنقل الملفات و المشاركة في القوائم البريدية حيث تفهرس المعلومات الموجودة على الشبكة ٠

١٠ - خدمة الاستعلامات واسعة النطاق

(WAIS) وهـــى تسمى بأسم حاسباتها الخادمة و هي اكثر دقة و فاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة

التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتوى على المعلومات المطلوبة ٠

١١ - خدمة الدخول عن بعد

(TEL NET) وهـــي خدمة تتيح استخدام أي برامج أو تطبيقات في حاسب آلي آخر

١٢ - الصفحة الإعلامية العالمية

(WORLD WIDE WEB) أو الويـــب (WEB) وهـــي تجمـــع كافة المـــوارد المـــتعددة التي تحتوى عليها الإنترنت للبحث عن كل ما في الشبكات المخـــتلفة و إحضــــارها بالنص و الصوت و الصورة و تعد الويب (WEB) نظامـــا فرعيا من الإنترنت لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة

مستلزمات الاتصال بالشبكة

ليتم الاتصال بالشبكة العالمية لابد من توافر عدة أشياء : -

١ - حاسب آلي

٢ - جهاز مودم

٣ - خط تليفون

٤ - الاشتراك في الخدمة

(في مصر و بعض الدول العربية اصبح الاشتراك في تلك الخدمة مجانا - فقط مقابل سداد مقابل الخدمة التليفونية)

٥ - وجود برامج تصفح شبكة الإنترنت ومن اشهرها

(INTERNET EXPLORER) (NETSCAPE)

جرائم الإنترنت

INTERNET CRIMES

تعتبر جرائم الإنترنت هي النوع الشائع الآن من الجرائم إذ أنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى ارتكابها ويمكن تعريف تلك الجرائم بأنها ((الجرائم التي لا تعرف الحدود الجغرافية CRIMES TRANS BORDER و التي يتم ارتكابها بأداة هي الحاسب الآلي COMPUTER عن طريق شبكة الإنترنت و بواسطة شخص على دراية فائقة بهما))

خصائص جرائم الإنترنت

CHARACTERISTICS OF INTERNET CRIMES

و تعتبر الجرائم التي ترتكب من خلال شبكة الإنترنت INTERNET CRIMES هي جرائم ذات خصائص CHARACTERISTICS متفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في اسلوبها و طريقة ارتكابها و التي ترتكب يوميا في كافة دول العالم و التي لها خصائص أخرى مغايرة تماما لخصائص تلك الجرائم التي ترتكب عبر الإنترنت وتلك الخصائص الخاصة بجرائم الإنترنت هي : -

١ - في جميع الأحوال يكون الحاسب الآلي هو أداة ارتكاب الجريمة

٢ - ترتكب تلك الجرائم عبر شبكة الإنترنت

٣ - أن مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلى

٤ - أن الجريمة لا حدود جغرافية لها

الخاصية الأولي :الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت
THE FIRST CHARACTERISTIC : THE COMPUTER IS THE COMMITTING UTENSIL OF THE IN TERNET CRIMES

خاصية أن الحاسب الآلي COMPUTER هو دائما أداة الجريمة في الجرائم التـــي ترتكب على شبكة الإنترنت هي خاصية متفردة عن أي جريمة أخرى ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الإنترنــت INTERNET و قـيامه بتنفـيذ جريمـــته أيا كان نوعها و عليه فالحاســب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت ٠

الخاصية الثانية : الجرائم ترتكب عبر شبكة الإنترنت
THE SECOND CHARACTERISTIC : CRIMES IS COMMITTING ACROSS THE INTERNET

تعـد شــبكة الإنترنــت INTERNET هــي حلقة الوصل بين كافة الأهداف المحـتملة لــتلك الجــرائم AIMS OF CRIMES كالبــنوك و الشــركات الصناعية و غيرها من الأهداف التي ما تكون غالبا الضحية لتلك الجرائم و هو مــا دعــا معظــم تلــك الأهــداف إلـــى اللجــوء إلـــى نظم الأمن الإلكترونية ELECTRONIC SECURITY SYSTEMS فـــي محاولة منها لتحمى نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائـــــم ٠

الخاصية الثالثة : مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي

THE THIRD CHARACTERISTIC :
THE CRIMINAL IS A PERSON HAVING A LOT OF EXPERIENCE WITH COMPUTERS

لاستخدام الحاسب الآلي COMPUTER لارتكاب جريمة على شبكة الإنترنت لابــد و أن يكون مستخدم هذا الحاسب الآلي على دراية فائقة و ذو خبرة كبيرة في مجال استخدامه وإلا فأين له بالخبرة اللازمة التي تمكنه من تنفيذ جريمته و العمــل على عدم اكتشافها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخــبراء في مجال الحاسب الآلي و أن الشرطة تبحث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب الجرائم

الخاصية الرابعة : الجريمة لا حدود جغرافية لها

THE FOURTH CHARACTERISTIC :
THE CRIME HAVE NO BORDER

شــبكة الإنترنــت ألغــت اي حــدود جغرافية فيما بين الدول و بعضها إذ يمكن الــتحدث فيما بين أشخاص ليس في بلدان مختلفة و إنما في قارات مختلفة في نفــس الوقت على شبكة الإنترنت من خلال الدردشة (SHATING) و عليه فأن أي جرائم ترتكب عبر شبكة الإنترنت INTERNET CRIMES فأنها تــتخطى حدود الدولة التي ارتكبت فيها لتتعدى آثارها كافة البلدان على مستوى العالم ٠

أهداف الجرائم الإلكترونية

AIMS OF ELECTRONIC CRIMES

ومن المعروف أن اكثر الجرائم الإلكترونية التي يتم ارتكابها يكون الهدف الأساسي لها هو الحصول على المعلومات الإلكترونية التي تكون اما محفوظة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت الا ان ذلك لا يعني أن هناك جرائم أخرى يكون لها هدف آخر غير الحصول على المعلومات مهما كانت أهمية تلك المعلومات و عليه فسوف نعرض لأهداف الجرائم الإلكترونية .

١ – المعلومات INFORMATION

هناك العديد من الجرائم التي يكون ارتكابها لهدف يتعلق بالمعلومات و يتمثل هذا الهدف أما بالحصول على المعلومات أو تغييرها أو حذفها نهائيا و هذا الهدف تعرضنا له تحت عنوان أمن المعلومات .

و معظم تلك الجرائم التي يكون الهدف منها المعلومات هي في الأغلب الأعم من الحالات تكون جرائم اقتصادية للحصول على مزايا أو مكاسب اقتصادية فالحرب الاقتصادية لا تقل في ضراوتها و شدتها حاليا عن الحرب العسكرية إلا انه تتم عبر شبكة الإنترنت .

٢ – أجهزة الكومبيوتر

أما عندما يكون الهدف من ارتكاب الجرائم الإلكترونية عبر شبكة الإنترنت هو أجهزة الكومبيوتر فالغالب يكون الهدف هو تخريب تلك الأجهزة نهائيا او على

الأقــل تعطــيلها لأطــول فترة ممكنة و معظم تلك الجرائم تتم بواسطة استخدام الفيروسات ٠

٣ – الأشخاص أو الجهات

معظــم الجرائم التي ترتكب عبر شبكة الإنترنت تستهدف اما اشخاص أو جهات بعينها و غالبا ما تكون تلك الجرائم هي جرائم مباشرة ترتكب في صورة ابتزاز أو الــتهديد أو التشــهير أو هي جرائم غير مباشرة ترتكب في صورة الحصول علــى البيانات و المعلومات الخاصة بتلك الجهات أو الأشخاص و ذلك لاستخدم تلك المعلومات و البيانات بعد ذلك في ارتكاب جرائم مباشرة ٠

أضرار جرائم الإنترنت
DAMAGES OF INTERNET CRIMES

وقــد أجريت عدة دراسات عن جرائم الإنترنت INTERNET CRIMES مــنها تلك الدراسة التي أجرتها منظمة (BUSINESS SOFTWARE ALLIANCE) في الشرق الأوســط والتي أظهرت أن هناك تباين بين دول الشــرق الأوســط فــي حجم خسائر DAMAGES جرائــم الإنترنت و جرائم الحاســب الآلــي حيــث تراوحــت بين ثلاثين مليون دولار أمريكي في المملكة العربــية الســعودية و الإمارات العربيــة المتحدة و مليون و أربعمائــة ألــف دولار أمريكي فقد في لبنان ٠

وقد أظهرت دراسة أخرى أجرتها هيئة الأمم المتحدة حول جرائم الإنترنت أيضا حوالي أربعون في المائة من منظمات القطاع العام و الخاص على السواء كانت ضحية لجرائم الإنترنت INTERNET CRIMES والحاسب الآلي ٠

وقـــد قدرت الولايات المتحدة الأمريكية اضرار جرائم الإنترنت DAMAGES OF INTERNET CRIMES و الحاســب الآلــي التــي تكبدتها حوالي خمسة مليارات دولار سنويا كما قدرت المباحث الفيدرالية الأمريكية (F.B.I) أن تكلفة جريمة الحاسب الآلي أو الإنترنت الواحدة حوالي ستمائة ألف دولار ســنويا مقــابل مبلغ ستة آلاف دولار تكلفة من جرائم السرقة بالإكراه و بينت دراسة أخرى أجراها أحد مكاتب المحاسبة الأمريكية أن حوالي مائتين و أربعون شــركــة أمريكــية قــد تضـــررت مـــن جـــرائم الغش باستخدام الكومبيوتر (COMPUTER FRAUD) و أظهـــرت دراســـة أخـــرى أجريت من قبل مـــنظمة (THE COMPUTER SECURITY INSTITUTE) عام ١٩٩٩ م أن خسائر حوالة مائة و ثلاثة و ستون شركة أمريكية من جرائم الحاســب الآلـــي و الإنترنــت قد بلغت اكثر من مائة و ثلاثة و عشرون مليون دولار فـــي حيـــن أن الدراسة التي أجريت في عام ٢٠٠٠ م قد أظهرت أن عدد الشـــركات التـــي تضررت قد ذاد إلى أن اصبح مائتان و ثلاثة و سبعون شركة تخطت خسائرها مبلغ مائتان و ستة و خمسون مليون دولار .

ومـــثال ذلك ما أعلنته شبكـــة أخبار (CNN) تحت عنوان طالب يسطو على المعهـــد الـــذي يدرس به جاء فيه أن سلطات ولاية تكساس تحقق مع طالب يدعـــى (فيليب اوستن) قد سطا إلكترونيا على المعهد الذي يدرس به حيث اســـتخدم كومبـــيوتر فـــي اقتحام أنظمة الكومبيوتر الخاصة بالمعهد حيث سرق بـــيانات خاصة بالضمان الاجتماعي و كذلك بيانات شخصيه و معلومات خاصة عـــن حوالي خمسه و خمسون ألف طالب و عضو بهيئة التدريس بالمعهد و قد قرر الطالب انه لم تكن لديه أي نوايا إجرامية و انه لم يكن يخطط لاستخدام تلك البيانات في أي أنشطة إجرامية .

وعلى ذلك فنتيجة الإحصائيات التي أجرتها الجمعية الأمريكية للأمن الصناعي

طبيعـــية عندما أعلنت أن الخسائر DAMAGES التي تسببها جرائم الحاسب الآلـــي و جرائم الإنترنت INTERNET CRIMES للصناعات الأمريكية قد تصل إلى حوالي ثلاث و ستون مليار دولار وان حوالي ٢٥ % من الشركات الأمريكية تتضرر من تلك الجرائم ٠

إثبات جرائم الإنترنت

و جرائم الإنترنت كثيرة و متنوعة و يصعب كشفها و حصرها و متابعة مرتكبها لان تلك الجرائم لا تترك أثرا يقود إلى مرتكبها مثل الجرائم التقليدية التي دائما ما تترك أثرا يقود إلى مرتكبها ٠

و تعــود أسباب صعوبة إثبات جرائم الحاسب الآلي و الإنترنت إلى خمسة أمور هم كالأتي :

- ١ – لا اثر للجريمة بعد ارتكابها
- ٢ – صعوبة الاحتفاظ الفني بآثارها أن وجدت ٠
- ٣ – أنها تحتاج إلى خبرة فنية و تقنية و يصعب على المحقق التقليدي التعامل معها ٠
- ٤ – أنهـــا تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبيها ٠
- ٥ – أنها تعتمد على قمة الذكاء و المهارة في ارتكابها ٠

ومـــع كـــل تلـــك المصـــاعب إلى تواجه إثبات جرائم الحاسب الآلي و الإنترنت PROVING THE INTERNET CRIMES ألا أن الأمـــر لـــيس بكل تلك الصعوبة ألا انه لا بد من الأخذ بعدة خطوات ليكون في الإمكان مكافحة

مثل تلك النوعية من الجرائم و تلك الخطوات هي : -

- ١ - تحديد الجريمة من البداية ٠
- ٢ - تحديد الجهة التي المنوط بها التعامل مع تلك الجرائم ٠
- ٣ - العمـل علـى تأهـيل عناصر تلك الجهات يكونوا على المستوى التقني الذي يمكنهم من العمل و مواجهة هذا النوع من الجرائم ٠
- ٤ - تعديـل القوانين بما يتناسب مع تلك الجرائم التي استجدت على و وضـــع العقـاب الشـديد لها لتكون مانعا من موانع ارتكاب مثل تلك الجرائـم ٠
- ٥ - التركـيز على مواجهة تلك الجرائم CRIMES بصفة دولية بإقـرار اتفاقات دولية تجرم تلك الجرائم و تعمل كل الدول على ملاحقة مرتكبيها ٠

فوائد شبكة الإنترنت للأمن

هذا من جهة و من جهة فأن شبكة الإنترنت INTERNET ليست فقط مرتعا لارتكاب الجرائم و إنما هي أيضا تقدم خدمات جليلة للأمن بصفة خاصة نوجزها كالآتي : -

- ١ - تلقى البلاغات بطريقة فورية و سريعة ٠
- ٢ - إضفاء نطاق من السرية فيما بين الأمن و المتعاونين معهم بمعنى عدم تعريض المتعاونين مع الأمن للخطر ٠
- ٣ - إعطــاء الفرصة لمن لديه معلومات من الجمهور أن يقدمها للأمن بطريقة سرية دون تعريض أمنه للخطر ٠

- ٤ – يمكـــن الأمـــن مـــن توسيع إطار البحث عن المجرمين بنشر صـــورهم وطلـــب الإبـــلاغ عن أي معلومات عنهم على الشبكة ليطلع علـــيها اكبر عـــدد ممكن مـــن الأشخاص لتضييق الخناق عليهم و يتم القبض عليهـــم .
- ٥ – وســـيلة لنشر أي معلومات أو بيانات أو قوانين أو قرارات جديدة تهم المواطنين .
- ٦ – فـــي بعـــض الـــبلاد يتم تكوين جمعيات أهلية – غير حكومية – مهمتها مساعدة الشرطة في مهام عملها و التواصل بين تلك الجمعيات و الشـــرطة عـــن طـــريق شبكة الإنترنت INTERNET يسهل من عملية التواصل بينهم و يفعل تلك المساعدة المقدمة من تلك الجمعيات إلى الشرطـــة .
- ٧ – إذا ما اصدر الأمن أي نشرات تتضمن توعية أو تعليمات للجمهور فـــأن نشـــر تلـــك النشرات على شبكة الإنترنت هي الطريقـــة المثلى لتوعية الجمهور بتلك النشرات وما تحتويه من تعليمات على المواطنين أن يلتزموا بها .
- ٨ – من خلال شبكة الإنترنت و ما عليها من مواقع تهتم بتوفير فرص العمـــل للشـــباب يمكـــن العمل على حل واحدة من أهم المشكلات التي تعترض عمليات التنمية في البلاد ألا وهى البطالة .
- ٩ – يـــتم اســـتخدام المواقع على شبكة الإنترنت في عمل الاستفتاءات علـــى جمـــيع القضـــايا ســـواء الوطنـــية أو العالمية و من خلال تلك الاســـتفتاءات يتم قياس مستوى رأى الجمهور فيما يعرض على القيادة السياسية من قضايا وطنية .
- ١٠ – تعتبر شبكـــة الإنترنت INTERNET بما تمثله من تقدم تقني

- MODERN TECHNIQUES من أهم أدوات التواصل فيما بين الشعوب و بعضها البعض و بالتالي يمكن استغلال هذا التواصل في نقل الـــتقدم التكنولوجـــي و العلمـــي بمعظم أنواعه من الدول المتقدمة إلى الـــدول النامـــية و العمـــل علـــى نقـــل التقدم الثقافي MODERN CALTURAL و العلمـــي أيضـــا و بالتالي تعتبر هذه الشبكـــة من أهـــم الطـــرق لـــرفع المستوى العلمي و التكنولوجي و الثقافي أيضا للشـــعوب النامـــية دون أن تكلفهـــا أي من الأموال الطائله التي كانت ســـتدفعها فيما لو طالبت تلك الدول المتقدمة مباشرة بهذه التكنولوجيا الجديـــدة و التي يمكنها الحصول عليها عبر شبكة الإنترنت و بدون أي مقابل مادي كما يمكنها أيضا من تدريب طلابها و علمائها عبر البرامج الدراســـية الكثـــيرة و المتخصصة عبر الإنترنت دون أن تتكلف مبالغ كثيـــرة .
- ١١ - تُعتـــبر الشبكة وسيطا فاعلا في عملية تدريب العاملين بمختلف المصـــانع و الشـــركات و تعريفهم بأحدث أساليب العمل في المصانع و الشركات المشابهة في الدول المتقدمة .

طرق ارتكاب جرائم الحاسب الآلي و الإنترنت

EXECUTION WAYS OF THE INTERNET CRIMES

ينمكـــن تقسم تلك الجرائم التي ترتكب عبر شبكة الإنترنت إلى أنواع بحسب ما تستهدفه من الجريمة و الطريقة في بلوغ هذا الهدف و على ذلك يمكن تقسيمها إلى أربع أنواع : -

النوع الأول TYPE 1

وهى الجرائم التي تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي (COMPUTER) لاستغلالها بطريقة غير مشروعة و يتميز هذا النوع من الجرائم بصعوبة اكتشافه .

النوع الثاني TYPE 2

وهذا النوع من الجرائم يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بما أو تدميرها كليا أو جزئيا و يمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني (E - MAIL) أو بواسطة برنامج (PROGRAM) مسجل في أحد الوسائط المتنوعة و الخاصة بتسجيل برامج الحاسب الآلي COMPUTER و يمكن اكتشاف هذا النوع من الفيروسات في معظم الحالات وذلك بواسطة برامج حماية متخصصة للبحث عن هذه الفيروسات و لكن يشترط الأمر تحديث قاعد بيانات DATA BASE برامج الحماية لضمان أقصي درجة من الحماية .
مع الوضع في الاعتبار أن وجود مثل هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وان ما من سبيل للوقاية إذا ما كان الهجوم بفيروس حديث لم يتم اكتشافه بعد ولم يتم تجهيز برامج للحماية منه بعد .

النوع الثالث TYPE 3

و هو استخدام الحاسب الآلي (COMPUTER) في ارتكاب الجريمة وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز يانصيب حيث قام أحد الموظفين بالشركة بتوجيه الحاسب الآلي

لـــتحديد رقــم معيــن كان قد اختاره هو فذهبت الجائــزة لشخص بطريقة غير مشروعـــــة ٠

النوع الرابع TYPE 4

و تشــمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه و مثال ذلك استخدام الموظف الحاسب الآلي في أمور خاصة لا تختص بالعمل بعد انتهاء وقت العمل ٠

الفصل الثاني

أنواع الجرائم التي ترتكب عبر شبكة الإنترنت
TYPES OF INTERNET CRIMES

نستعرض الآن الجرائم التي ترتكب على شبكة الإنترنت ماهيتها و وصفها القانوني و وسائل مكافحتها وهى كالآتي :

١ – الجرائم و الممارسات الجنسية و غير الأخلاقية

- المواقع الإباحية
- مواقع قذف و تشويه سمعة الأشخاص
- الدخول إلى المواقع المحجوبة
- إخفاء الشخصية
- انتحال الشخصية
  - انتحال شخصية الفرد
  - إنتحال شخصية المواقع

٢ – جرائم الاختراق

- الاقتحام أو التسلل
- الإغراق بالرسائل
- فيروسات الحاسب الآلية
  - خطورة برنامج حصان طروادة
  - أهم المنافذ المستخدمة لاختراق الجهاز

٣ – الجرائم المالية

- جرائم السطو على أرقام البطاقات الائتمانية
- القمار عبر الإنترنت
- تزوير البيانات

- الجرائم المنظمة
- تجارة المخدرات عبر الإنترنت
- غسيل الأموال

٤ – المواقع المعادية

٥ – جرائم القرصنة

٦ – التجسس الإلكتروني

٧ – الإرهاب الإلكتروني

أولا : الجرائم و الممارسات الجنسية و غير الأخلاقية

١ – المواقع الإباحية
UNIHIBITED LOCATIONS

لقـد وفـرت شـبكة الإنترنت اكثر الوسائل فعالية و جاذبية لصناعة و نشر الإباحـيـة الجنسيـة فأن شبكة الإنترنت جعلت الإباحية بشتى وسائل عرضها من صور و فيديو و حوارات سواء كانت مسجله أو مباشرة في متناول الجميع و يعتبر ذلك من اكبر سلبيات شبكـة الإنترنت ٠

فـأن التأثـير على البلاد حاليا يكون من خلال التأثير على شبابها فهو الأساس الـذي ترتكـز علـيه الـبلاد فـي تحقيق نموها و طموحاتها و تهدف إليه في مسـتقبلها و علـيه و لمـا كانـت شبكة الإنترنت INTERNET هي شبكة مفـتوحة مليـئة بما هو مفيد ألا أنها أيضا مليئة بكل ما هو محرم و مرفوض طبقا لديننا و طبقا لتقاليدنا الشرقية ٠

ولمـا كانـت المواقع الجنسية الإباحية UNIHIBITED LOCATIONS الموجـودة بكثرة على شبكة الإنترنـت تريد تحقيق الكثير من المكاسب المادية عـن طريق زيادة مرتاديها فأنها تشترط دفـع مبالغ مالية مقابل الحصول على خدماتها المتمثلة في عرض و تحميل الأفـلام البورنو الإباحية فأنها تحاول ذلك عـن طـريق إعطـاء مرتادي تلك المواقـع العديد من الصور الجنسية بلا أي مقابل مادي لتحاول جذب من يرتاد تلـك المواقـع إليها ٠

وزيـادة علـى ذلك فأن تلك المواقع الإباحية تحاول في كل وقت تسهيل عملية الدخول على مواقعها و كذلك تسهيل عملية الحصول على ما تقدمه من برامج و أفلام و صور إباحية لمرتاديها ٠

وقد يبدو للبعض أن تلك المشكلة هي مشكلة محلية خاصة بنا في منطقة الشرط الأوسط على أساس أن عاداتنا و تقاليدنا ترفض ذلك و تحرمه ألا أن تلك المشكلة هي مشكلة عالمية تحاول كل الدول كل بطريقتها مقاومة تلك المشكلة والحد من آثارها ٠

ومثال ذلك التقرير الذي نشرته شبكة (C N N) الإخبارية بتاريخ ١٥ / ٣ / ٢٠٠٣ في موقعها على شبكة الإنترنت (WWW.CNN.COM) بعنوان - سهولة الوصول إلى الملفات الإباحية - ذكرت فيه أن الوصول الآن إلى الملفات الإباحية اصبح بنفس السهولة التي يمكن الوصول بها إلى ملفات الموسيقى (M P 3) و أنه يمكن أيضا تحميل الملفات الإباحية بنفس السهولة عند تحميل ملفات الموسيقى (M P 3) وان ذلك يتم بالرغم من كافة الإجراءات التكنولوجية التي تم اتخاذها للحد من ذلك ٠

وقد ذكرت الشبكة في تقريرها أن هذا الموضوع الهام منظور حاليا أمام لجنة إصلاح حكومية أمريكية بهدف معالجة تلك الظاهرة والحد منها ٠

أما القوائم البريدية فهي اسهل إنشاء و غالبا ما تكون مجانية و يقوم أعضائها من المشتركين بتبادل الصور و الأفلام الإباحية على عناوينهم البريدية و يشترك في القوائم البريدية آلاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعنى كم هائل من الصور و الأفلام الإباحية يتبادلها مشتركي القوائم البريدية بشكل يومي ٠

و يوجد على الإنترنت حاليا آلاف المواقع الإباحية الجنسية و التي أصبحت اكثر تخصصية فمنها من هو متخصص في أفلام الفيديو و منها من هو متخصص في الصور و الكثير منها متخصص في برامج المحادثة (CHATTING) و للأسف فأن كل تلك الأنواع من المواقع تجد الكثير جدا من الإقبال على زيارتها و تصفح محتوياتها الإباحية ٠

وفـــي دراســـة أجـرتها شبكة (B B C) عام ١٩٩١ م أن معدل التدفق على زيـــارة تلـــك المواقع الإباحية في أوقات العمل و التي تبدأ من الساعة التاسعة صـــباحا و حـــتى الخامسة عصرا تمثل حوالي ٧٠ % من إجمالي نسبة التدفق على زيارة تلـــك المواقـــع ٠

و كشـــفـــت دراســـــة أخرى أجراها الدكتور / مشعل القدهى – بأن هناك إقبالا كبيرا على زيارة تلك المواقع الإباحية UNIHIBITED LOCATIONS حيـــث ذكـــرت شركة (PLAY BOY) الإباحيـــة و التي تصـــدر مجلـــة إباحـــية بـــنفس الاسم بأن ٤,٧٠ مليـــون زائر يزورون صفحاتها على شبكـــة الإنترنـــت أســـبوعيا وان هنـــاك بعـــض الصفحات الإباحية المشابـــهة تستقبل اكـــثر مـــن ربـــــع مليون زائـــر يوميا كما وجـــد أن اكثـــر مـــن (٨٠ %) ثمانين في المائـــة من الصـــور المتداولة في المجموعات الإخبارية هي صـــور إباحـــية و أن اكـــثر مـــن ٢٠ % عشرون بالمائـــة من سكان الولايات المتحدة الأمريكيـــة يزورون تلـــك الصفحات الإباحية حيـــث تبدأ زيارة تلـــك المواقع LOCATIONS أولا بهدف الفضول و معرفـــة محتوياتها ثم يتطور الأمـــر فـــيما بعد إلى الإدمان على زيارة تلك المواقع وهـــو ما تستغله تلك المواقع في وضـــع رســـوم يجب سدادها أولا قبل السماح بالدخول إلى الموقـــع و مشاهدة و تحمـــيل ما يحتويـــه من ملفات الأفـــلام و الصور الإباحية وهـــو ما يحقـــق لها أرباح خياليـــة ٠

ويؤكد ذلك ما نشر من أن مجموع مشتر وات المواد الإباحية من شبكة الإنترنت فـــي عام ١٩٩٩ م ما نسبته ٨ % من دخل التجارة الإلكترونية البالغ ١٨ مليار دولار أمريكـــي فـــي حيـــن بلـــغ مجموع الأموال المنفقة للدخول على المواقع الإباحيـــــة UNIHIBITED LOCATIONS ما قيمته (٩٧٠) مليون

دولار أمريكـــي و وصـــل المبلغ في عام ٢٠٠٣ م إلى حوالي ثلاثة مليار دولار أمريكي .

ومن جهة أخرى فقد أوضحت دراسات أجريت أن اكثر زوار المواقع الإباحية هم مـــن الشـــباب التي تتراوح أعمارهم بي (١٢) و (١٥) عاما في حين تمثل الصفحات الإباحية اكثر صفحات الإنترنت طلبا .

كما أوضحت دراسة أجرتها (ADSIT - 1999) أن المواقع الإباحية أضحت مشـــكلة حقيقـــية وان آثارهـــا تطول كافة المجتمعات دون أن تعوقها أي حدود جغرافيـــــة .

وقـــد جرى حصر المواقع الإباحيـــة العربية ARABIC UNIHIBITED SITES فقـــط دون الأجنبية في بعض المواقع على شبكـــة الإنترنت و منها موقـــع (YAHOO) فوجد أنها تصل إلى (١٧١) موقع بلغ عدد أعضاء اقلها إلى (٣) في حين بلغ عدد أكثرها أعضاء إلى (٨٦٨٣) عضوا و العدد في ازدياد .

وأخيرا لابد من الربط بين زيارة مثل تلك المواقع الإباحية الخليعة و التي تضغط علـــى الغرائز و تثيرها في مجتمعات محافظة جنسيا كالمجتمعات العربية و بين زيادة الجرائم الجنسية التي زاد عددها .

التكييف القانوني للجريمة

الإباحـــية الجنسيـــة هي أمر مجرم في كافة القوانين العربية بل و في الكثير من القوانين في معظـــم بلاد العالـــم و تندرج تحت جريمة مسماها : -

((إتيان الأعمال الفاضحة علنية و التحريض على ممارستها))

و يعد من الأمور المشددة في التجريم أمرين هما : -

- ١ - العلنية أثناء ممارسة هذا الفعل
- ٢ - العلانية في التحريض على ممارسته

و مثال ذلك ما هو منصوص عليه في قانون العقوبات المصري من تجريم لتلك الأفعال و عقاب من يقوم بها ٠

إذ ينص قانون العقوبات المصري في مواده على معاقبة

- كل من وجد في الطريق العام أو مكان مطروق يحرض المارة على الفسق بإشارات أو أقوال ٠

المادة ٢٦٩ مكرر

- كل من فعل علانية فعلا فاضحا مخلا بالحياء ٠

المادة ٢٧٨

و لما كانت شبكة الإنترنت INTERNET تعد مكانا مطروقا من الكثير من الشخصيات بل أنها مطروقة من أشخاص من كافة الجنسيات على مستوى العالم وهو ما يجعلها تحمل نفس خصائص الطريق العام أو المكان المطروق المنصوص عليهما في قانون العقوبات المصري ٠

كما أن شبكة الإنترنت تحمل صفة العلنية بمعنى أن من يقوم بفعل على الشبكة يكون بإمكان أي من مرتادي الشبكة الاطلاع عليه ٠

و لما كانت المواقع الإباحية UNIHIBITED LOCATIONS المنتشرة على شبكة الإنترنت INTERNET هي مواقع تحرض على الفسق و الأكثر من ذلك أنها لا تحرض على الفسق فقط بالإشارة و القول و إنما اكثر من ذلك فهي تحرض على الفسق بالصور و أفلام البورنو – الجنس - وهو الفعل الذي تم النص عليه في المادة[1] (٢٦٩) من قانون العقوبات المصري ٠

بل أن المحادثات الجنسية التي تتم غالبا من خلال ما يعرف بغرف المحادثات

(CHATTING) تنـدرج تحـت فعـل الأفعال الإباحية الفاضحة التي تتم علانية و التي تم النص على تجريمها طبقا للمادة (٢٧٨) من قانون العقوبات المصري ٠

هـذا مـن جهـة و مـن جهـة أخرى فان كافة القوانين العربية تتعرض لذات الموضـوع و لا اخـتلاف بيـنها في ذلك فكافة القوانين العربية قد جرمت تلك الأفعال المخالفة لتعاليم كافة الأديان السماوية ٠

٢ – مواقع قذف و سب و تشويه سمعة الأشخاص

مـع انتشـار الشائعات و الأخبار الكاذبـة والتي تطول و تمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسيـة حتى أنها طالت الرموز الدينية أيضا ظهـرت علـى شـبكة الإنترنت بعض المواقع المشبوهة و التي جنـدت نفسها لهـدف واحـد هو خدمة تلك الشائعات و الأخبار الكاذبة و ذلك بهدف قـذف و سـب و تشـويه سـمعة تلك الرموز السياسية و الفكرية و حتى الدينية والتي تلـتـف حولهـا الشعوب و الهدف الأساسي من تلك المواقع هو كما ذكرنا هو تشـويـه تلـك الرموز بهدف تشكيك الناس في مدى مصداقية هؤلاء الأفراد و محاولـة فـض الناس من حولهم ليخلوا لهم الجو في محاولة منهم لتسميم أفكـار الناس ٠

هذا من جهة و من جهة أخرى فقد يكون الهدف من تلك المواقع محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم إذا لم يرضخوا و يدفعوا مقابل مادي لعدم التعرض لهم و تركهم دون تشويه سمعتهم ٠

و مـثال ذلك ما حـدث في بداية دخول الإنترنت جمهورية مصر العربية عندما فسخت فتاة خطبتها من شاب و لرغبتـه في الانتقام منها لفسخ خطوبتها منه

صـــمم موقعــا على شبكة الإنترنت INTERNET و خصصه لنشر الأكاذيب عــن تلــك الفتاة و عن فساد أخلاقياتها و دينها و الأكثر من ذلك أنه قام بنشر أرقــام تلــيفوناتها و مكـــان عملها و بدأت الفتاة في تلقى مكالمات سيئة من أشـــخاص مجهولين طالعوا ذلك الموقع LOCATIONS و قاموا بالاتصال بهـــا تأسيســـا علـــى المعلومات المنشورة في الموقع مما حدا بالفتاة إلى إبلاغ الشـــرطة التي قامت بتحرياتها التي أثبتت كذب تلك المعلومات التي نشرت بذلك الموقع و بدأت في تتبع ذلك الشخص الذي نشر تلك المعلومات على هذا الموقع إلى أن أثبتت التحريات أن مصمم ذلك الموقع هو خطيبها السابق بغرض الانتقام منها لفسخها خطبتها منه ٠

وعلـــيه فهذا مثال على موقع صمم بهدف واحد هو سب و قذف و تشويه سمعة فتاة لا لهدف إلا لأنها فسخت خطبتها ٠

و مثال آخر عندما تمكن المباحث في جمهورية مصر العربية من ضبط مهندس كومبـــيوتر مصـــري بـــتهمة نشر معلومات كاذبة على الإنترنت للتشهير بعائلة مســـئول مصـــري و عائلـــته و ابنـــته و تصـــميم موقـــع CREATE LOCATIONS على شبكة الإنترنت لهذا الغرض ٠

و أشـــارت الصحف إلى أن ابنة المسئول المصري كانت عرضة للتشهير بعد أن قام أحد الأشخاص بنشر موقع على شبكة الإنترنت باستخدام بيانات عن الضحية بغرض التشهير بها

و أن إدارة مكافحـــة جـــرائم الحاســـبات و شـــبكات المعلومات بوزارة الداخلية المصـــرية قـــد تمكنت بالتنسيق مع المباحث العامة في ضبط الشخص الذي قام بالتشـــهير بابـــنة المسئول الكبير و البالغة من العمر ثمانية عشر عامل و نشر معلومـــات كاذبة حولها بهدف الإساءة إلى سمعتها و سمعة عائلتها و تبين بعد التحريات و المتابعـــة الإلكترونيـــة التي قامت بها أن إدارة مكافحة جرائم

الحاسبات و شبكات المعلومات بوزارة الداخلية – وهي إدارة جديدة تم إنشائها حديــثا بوزارة الداخلية المصرية لمواجهة تلك الجرائم الإلكترونية الجديدة على المجــتمع المصــري - للشخص الذي قام بإنشاء ذلك الموقع CREATE SITE المســيء أن المــتهم هو مهندس كومبيوتر و مصمم برامج و انه أنشا الموقــع و المعلومــات الملفقــة بغرض التشهير و قد ضبطت الأجهزة الأمنية الشــخص و تحفظــت علــى جهاز الكومبيوتر المستخدم لكونه دليلا ماديا على ارتكاب تلك الجريمة الإلكترونية .

كمــا أن هــناك حادثة أخرى مشهورة جرى تداولها بين مستخدمة الإنترنت في بداية دخول الخدمة في منطقة الخليج حيث قام شخص في دولة خليجية بإنشاء موقــع على شبكة الإنترنت INTERNET نشر فيه صور لفتاة و هي عارية مــع صــديقها و كان قد حصل على تلك الصور بعد التسلل إلى جهاز الحاسب الآلــي الخــاص بتلك الفتاة و نسخ منه تلك الصور و لما حاول ابتزازها جنسيا بتلك الصور و رفضت قام بإنشاء ذلك الموقع و نشر فيه تلك الصور مما أدى بالفتاة إلى أن تنتحر بعد ما سببه لها من فضيحة بين أهلها و ذويها .

كمــا وقعــت حادثـــة تشـــهير أخرى من قبل تصدى له من اسموا أنفسهم ((الأمجــاد هكــرز)) حيــث اصــدروا بــيان نشر على الإنترنت بواسطة البريد الإلكترونــي ووصـــل للعديــد من مشتركي الإنترنت أوضحوا فيه قيام شخص بالتطاول في أحد المنتديات بالسب و القذف على شيخ الإسلام ((ابن تيميه)) و غــيره مــن رموز الفكــر الإسلامي الذي يلتف حولهم المسلمون لمعرفة أمور ديــنهم و دنــياهم و قد استطاع من اسموا أنفسهم ((الأمجاد هكرز)) اختراق الــبريد الإلكتروني لهذا الشخص الذي قام بالتطاول على رموز الإسلام و من ثم تــم نشــر صوره و كشف أسراره في موقعهم على الإنترنــت لتجرئه على ما ارتكب في حق رموز الإسلام .

التكييف القانوني للجريمة

تعـد جريمة السب و القذف و التعرض للحياة الشخصية للأفراد بغرض التشهير و الخـوض فـي أعراضهم من اكبر الجرائم التي تم تجريمها في كافة القوانين سواء في الدول العربية أو الدول الأجنبية يا كانت الطريقة أو الوسيلة التي تتم بهـا تلك الجريمة سواء كانت تتم بالطرق التقليدية أو بالطرق الحديثة التي تتم باسـتخدام شـبكة الإنترنـت بواسـطة إنشـاء مواقـع CREATE LOCATIONS خاصـة بقـذف و سب و التشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان ٠

و أسـباب ذلـك الـتجريم تنطوي على أن الحرية و الديمقراطية التي تنعم بها الشـعوب لا يجب أن تنطوي على الإخلال بها و تجريح الأشخاص في أعراضهم و مـبادئهم و شـرفهم و نسـب أمور غير صحيحة لهم بغرض التشهير بهم و بمـبادئهم و الخـوض في أعراضهم و في حياتهم الخاصة التي هي ملك لهم و حدهـم دون أن يكون لأي شخص آخر أن يخوض أو يتدخل فيها بأي شكل من الأشكال ٠

و يمكـن حصـر الأمـور المجـرمة قانونا في جرائم القذف و السب التي تقه بالطرق التقليدية في الآتي : -

- إسناد أمور لو كانت صحيحة لأوجبت عقاب من تم إسناد هذا الأمر إليه أو احتقاره عن أهله ٠
- أي سب بحيث يكون متضمنا خدشا للشرف أو الاعتبار
- التعرض لأنثى على وجه يخدش حيائها
- التعرض لحرمة الحياة الخاصة

و يمكن حصر الأمور المشـددة للعقاب إذا ما ارتكبـت الجرائـم سالفـة الذكر في الآتي : -

- إذا ما كان من تم سبه و قذفه موظفا عاما
- إذا مـا تمـت واقعة القذف و السب بطريق النشر في إحدى الجرائد أو المطبوعات
- إذا ما تمت واقعة القذف و السب بطريق التليفون
- إذا مـا كـان القـائم بتلك الجريمة من تعرف على تلك الأمور بمناسبة قيامه بعمله كالصيادلة و الأطباء و غيرهم

و عليه فأن جريمة القذف و السب و التشهير التي تتم بالطرق الحديثة التي تتم باستخدام شبكة الإنترنت بواسطة إنشاء مواقع يكون هدفها فقط قذف أو سب أو التشـهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان تقع تحت طائلـة نفـس النصـوص القانونـية التي تجرم تلك الأفعال متى تمت بالطرق التقليدية ٠

وفى القانون المصري فقد تم تجريم تلك الأفعال و تم النص في قانون العقوبات المصري على تجريم تلك الأفعال في المواد من المادة (٣٠٢) و حتى المادة (٣١٠) ففـي المادة ٣٠٢ من قانون العقوبات المصري تم النص على انه يعد قاذفـا كل من اسند لغيره أمورا لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبـات المقررة قانونا أو أوجبت احتقاره عند أهل وطنه و قد تم النص في المـادة ٣٠٣ علـى العقوبة PUNISHMENT المقررة في حالة ارتكاب تلـك الجريمة بالحبس مدة لا تتجاوز سنتين و بغرامة لا تقل عن عشرين جنيها و لا تزيد عن مائتي جنيه أو بإحدى هاتين العقوبتين فقط ٠

و يلاحـظ هنا ضعف العقوبة PUNISHMENT المقررة على تلك الجريمة

CRIME و ذلــك علــى اعتبار أن ارتكاب تلك الجريمة في البيئة الاجتماعية المصرية قليل للغاية و انه يعد من اندر الحوادث على الإطلاق حيث أن العادات و التقالــيد المصــرية و العربية بصفة عامة تعمل على الارتقاء بالنفس و عدم إهانة الأشخاص مهما كانت درجة الاختلاف في الرأي ٠

بــل أن المادة ٣٠٥ من ذات القانون قد نصت على أن من اخبر بأمر كاذب مع سوء القصد فيستحق العقوبة ولو لم يحصل منه إشاعة ٠٠٠٠٠٠

أما المادة ٣٠٦ فقد نصت على أن كل سب لا يشتمل على إسناد واقعــة ومعينه بــل يتضــمن بــأي وجــه من الوجــوه خدشا للشرف أو الاعتبار يعاقب عليه بالحبس مدة لا تجاوز سنــة و بغرامة لا تزيد على مائتي جنيه أو بإحدى هاتين العقوبتين ٠

٣ – الدخول إلى المواقع المحجوبة

بعــض الدول تعمل على حجــب المواقــع LOCATIONS غير المناسبة و المتماشــية مع تقاليدها الاجتماعية و مثال ذلــك أن بعــض الدول تعمل على حجب المواقع الجنسية الإباحيــة حتى لا يستطيع زائري شبكة الإنترنت الدخول إلــى تلــك المواقــع و تلـــك الــدول تعمــل على حمايــة تقاليدها و عاداتها الاجتماعــية ممــا يمكــن أن يســببــه الدخــول علــى تلك المواقــع الإباحية UNIHIBITED LOCATIONS ألا أن بعــض الأشخاص يعملون على الدخــول إلــى تلـــك المواقــع بالرغــم من حجبها باستخدام بعض البرامج المتخصصــة فــي الدخــول إلى المواقــع المحجوبة و هؤلاء الأشخاص بذلك يرتكــبون جــريمــة يــنــص عليها قانون الدولــة التي تعمل على حجب تلك الواقــع ٠

وعلـيـه فأن هؤلاء الأشخاص عندما يستخدمون بعض البرامج بغرض الدخول إلـى تلـك المواقع المحجوبة يعتبرون مرتكبي جريمة الدخول إلى تلك المواقع على أساس أن قوانين تلك الدول التي تحجب تلك المواقع تجرم الدخول إلى تلك المواقع .

و نحـن نرى أن حجب تلك البرامج هو تصرف صحيح بالنسبة إلى الأطفال اقل من السن التي يمكن أن يؤثر فيهم تلك المواقع و يستطيعون الفرار من تأثيرها الـذي قـد يعتبر مميتا على المحافظة على تعليمات الدين و العادات و التقاليد الاجتماعية السائدة في تلك الدول .

التكييف القانوني للجريمة

الكثـير من البلاد لا يتم إدخال خدمة الإنترنت بها إلا بعد إجراء ما يسمى بفلترة المواقـع أي أن الدولـة تقوم بحجب بعض المواقع التي تجد أنها غير مناسبة للدخول عليها سواء لأسباب دينية أو سياسية و عليه فهى تقوم بفلترة المواقع و حجـب مـا ترى انه غير مناسب بحيث لا يكون من الممكن الدخول إلى تلك المواقع و عليه فالدخول إلى تلك المواقع في تلك البلاد تعد جريمة يعاقب عليها القانون .

و الدخول إلى تلك المواقع المحجوبة لا يكون مستحيلا على من يريد الدخول إذ توجـد الـبرامج المتخصصة في ذلك و التي تمنع عملية الحجب التي تقوم بها الدولة .

و نحـن هـنا في مصر لا توجد أي مواقع محجوبة فالدولة تنتهج سياسة ترك الإنترنـت دون أي حجب و تعمل في نفس الوقت على زيادة التوعية الدينية و الثقافية لأفراد الشعب .

٤ – إخفاء الشخصية

نظــرا للــتطور الهائل في مجال البرمجيات على مستوى العالم و الذي نشهده الــيوم و الــذي يــزداد كــل فــتــرة قصــيــرة فقــد ظهرت بعــض البرامج المتخصصة SPECIAL PROGRAMS التي يمكن استخدامها في إخفاء هوية الشخص عند الدخــول على شبكة الإنترنت INTERNET و لكن غالبا مــا يــتم استخدام برامج PROGRAMS إخفاء الشخصية تلك عند الدخول على برامج التحدث CHATING PROGRAMS حتى يتمكن الشخــص مــن الــتحدث كمــا يــريد و في المواضيع التي يريدها دون إعلان شخصيته الحقيقــية كــي لا يــتعرف عليــه أحد و هو ما يمكنه من التحــدث في برامج الــتحدث CHATING PROGRAMS دون الــتزام بتقالــيد أو بقوانين LAWS وهــو مــا يخجــل مــن الحديــث فــيه في حالة ما إذا لو عرفــت شخصيتــه الحقيقية و كذلــك عند إرسال البريد الإلكتروني SENDING E - MAIL - حــتى لا يعــرف المرســل إليه هــذا البريد الإلكتروني مــن هــو المرســل ممــا يمكـــن المرســل من أن يرســل أي شئ وقــح أو مخالــف للقوانين دون الخوف من أن ينال عقاب ما فعلــه .

ألا انــه و مع تقدم البرامج المتخصصة SPECIAL PROGRAMS فقد أمكــن الــتعرف علـــى الشخص حتى ولو حاول أن يخفى شخصيته ألا أن ذلك يتطلــب الكثير من الجهد و نتائجه ليست مضمونة مائة في المائة في الوصول إلى شخصية المتحدث على برنامج المحادثة (CHATING) أو مرسل البريد الإلكتروني .

وفى معظم الأحوال قد يمكن معرفة الرقم أو المكان الذي تمكن منه هذا الشخص من الدخول على الإنترنت منه دون معرفة بياناته الحقيقية التي أخفاها .

التكييف القانوني للجريمة

لا يعـد إخفـاء الشخصـية جريمة في قوانين جمهورية مصر العربية إلا إذا تم الاستفســار عـنها و لـم تتم الاجابة بصورة صحيحة فتعمد إخفاء البيانات من الظهـور علـى الإنترنـت لا يعد جريمة إلا انه في بعض البلاد الأخرى يعد هذا الاجراء جريمة يعاقب عليها القانون

٥ – إنتحال شخصية الفرد

تبدأ عملية انتحال الشخصية عبر الإنترنت عندما يستغل اللصوص بيانات شـخص مـا علـى الشـبكة الإلكترونية أسوأ استغلال ومن هذه البيانات العـنوان وتـاريخ المـيلاد ورقـم الضمان الاجتماعي وما شابه من أجل الحصول على بطاقات ائتمانية أو رخص قيادة و عليه يستطيع المجرمون من خلال هذه المعلومات أن يخفوا شخصياتهم الحقيقية ويتصرفون بحرية تحـت اسـم مسـتعار وتمكن أرقام الضمان الاجتماعي والبيانات الأخرى لصـوص انتحال الشخصيات من التقدم بطلبات لاستخراج بطاقات ائتمانية عـبر الإنترنت غالبا من خلال هيئات لا تتخذ الإجراءات الأمنية الصارمة عـبر الشبكة فإذا قام أحد لصوص انتحال الشخصية بصناعة تاريخ جديد لـه عـن طـريق تسديد فواتير شهرية بالبطاقة الائتمانية سوف يكون له الأحقـية فـي طلب قروض لشراء سيارات وإيجار العقارات وتشير هيئات وشـركات الـبطاقات الائتمانية من طرفها إلى أن نسبة انتحال الشخصية ضعيفـة جدا مقارنـة بمئات المليارات من الدولارات التي تنفق عبـر

البطاقات الائتمانية سنويا .

و جـريمة انـتحال الشخصـية جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية القديمة ألا انه و مع انتشار شبكة الإنترنت فقد اخذ هذا النوع من الجرائم شكلا جديدا مستفيدا من التطور التكنولوجي الذي تمثله شبكة الإنترنت INTERNET وغالبا ما يكون انتحال شخصية الشخص علـى شـبكة الإنترنت غالبا مه يكون بهدف أما تشويه سمعة هذا الشخص أو اسـتخراج بطاقـات ائتمانية أو الاستيلاء على بعض ممتلكاته أو كلها أن أمكن بحسب الشخص المراد انتحال شخصيته و مواقفه سواء السياسية أو الدينية أو درجـة ثـراءه و مـا إلـى ذلك من أسباب يتم من اجلها انتحال شخصية هذا الشخص .

و انـتحال شخصـية الشـخص يتطلب كما ذكرنا سلفا الحصول على الكثير من المعلومـات المتعلقة به و للحصول على تلك المعلومات يلجأ المنتحل إلى الكثير مـن الطـرق الملـتوية لمخاطبة هذا الشخص و الحصول من خلاله على تلك المعلومات أو أن يحاول اللجوء إلى وسائل إحتيالية أخرى بحيث يمكنه من خلالها الحصول على تلك المعلومات .

و غالـبا مـا يتحصـل المنتحل على تلـك المعلومات التي يريدها عن طريق اسـتغلال عـادة الطمع التي توجد دائما في الكثيـر من الأشخاص و غالبا ما يتم ذلك عن طريـق الكم الهائل من الإعلانات التي تزدحـم بها شبكة الإنترنت و التـي تخاطـب غالـبا غريزة الطمع في الإنسان في أن تمنيه بالفوز مثلا بجائـزة غالـية الثمـن أو كبيرة القيمة مقابل ثمن قليل لا يقارن بتلك الجائزة وغالبا ما يتم استغلال ذلـك في الوصول إلى الشخص المـراد انتحال شخصيته بهدف الحصـول منـه على أي معلومات تكون لازمة للمنتحل ليتمكن من إتمام عمليـة الانتحال .

و عملية انتحال الشخصيات هي جريمة مؤثمة و مجرمة قانونا في الكثير من الدول طبقا للقوانين التقليدية دونما احتياج إلى تعديل تلك القوانين لتستوعب تلك الجريمة فانتحال الشخصية هي جريمة قديمة AN OLD CRIMES فقد أصبحت تتم بأسلوب متطور تكنولوجيا دون الأسلوب الذي كانت تتم به قديما هذا بالنسبة إلى الأسلوب أما الجريمة نفسها فهي مجرمة نظرا لما يكابده الشخص الذي تم انتحال شخصيته من أضرار اقلها الأضرار المعنوية بجانب الأضرار المادية حيث أن انتحال الشخصية لا يتم ألا لقذف و سب هذا الشخص أو تشويه سمعته أو للحصول على بعض أو كل ما يملكه ٠

التكييف القانوني للجريمة

اختلاس الألقاب و الوظائف و الاتصاف بها دون حق هي جريمة مؤثمة و مجرمة في القانون المصري و في كافة القوانين العربية ٠

إلا أن تلك الجريمة التي ترتكب عبر الإنترنت تكون غالبا مقترنة بجريمة أخرى أما سرقة بيانات أو عمليات نصب و احتيال أو الاستيلاء على أملاك الغير أو ما إلى ذلك من جرائم أخرى غالبا ما تكون مقترنة بجريمة انتحال الشخصية ٠

و تلك الجرائم المقترنة هي جرائم مؤثمة و مجرمة قانونا أيضا إلا أنها تعد عاملا مشددا للعقاب في جريمة انتحال الشخصية إذا ما اقترنت بها ٠

و قد نص قانون العقوبات المصري على تلك الجرائم في المواد من ١٥٥ – ١٥٩ إلا انه يؤخذ على المشرع المصري ضعف العقوبة المقررة على تلك الجرائم رغم أهميتها و ما يترتب عليها من أضرار هامة سواء مادية أو أضرار معنوية للشخص التي تمت انتحال شخصيته ٠

و نحــن نرى أن المشرع المصري عليه أن يشدد كثيرا في العقاب المقرر على تلك الجرائم لما يترتب عليها من أضرار مادية و معنوية كبيره تؤثر اشد التأثير على الشخص الذي تم انتحال شخصيته ٠

٦ – إنتحال شخصية المواقع

و إنتحال شخصية المواقع تعنى انه يمكن لبعض الأشخاص الدخول على الموقع و إمـــا أن يحجبه و يضع الموقع الخاص به بدلا منه أو أن يغير هذا الموقع كما يحلـــوا له ويحـــدث هذا في غالب الأحيان في المواقع السياسية أو الدينية وذلك لاسباب دينية أو سياسية ٠

ففـــي المواقـــع السياســـية نـــرى هـــذا يحـــدث فيما بين المواقع الفلسطينية PALESTINIAN SITES و المواقـــع الإســـرائيلية فكثـــيرا مـــا يدخـــل الفلســـطينيون علـــى المواقـــع الإسرائيلية و يقوموا بإلغاء الصفحة الرئيسية و يضـــعون بدلا منها العلم الفلسطيني و العكس بالعكس نرى انه يحدث أيضا أن يدخـــل بعـــض الـــيهود الإســـرائيليين إلـــى بعـــض المواقـــع الفلســـطينية PALESTINIAN SITES و يحـــاولون إلغـــاء الموقع و وضع بدلا منه صورة العلم الإسرائيلي و النشيد الوطني الإسرائيلي ٠

و انتحال المواقع هذا لا يحدث بين الإسرائيليين و الفلسطينيين فقد و إنما يحدث فيما بين كل طرفين بينهما أي مشكلة سياسية أو دينية فليست الحروب الحديثة كلهـــا تدور الآن بالدبابات و الطائرات و إنما الكثير منها ألان يدور على أجهزة الكومبـــيوتر و علـــى شـــبكة الإنترنـــت فسلاح الكومبيوتر اصبح الآن من أهم الأســـلحة التـــي تستخدم في المعارك نظرا لتأثيرها البالغ الأهمية على المعركة الإعلامية التي يدور رحاها بجانب المعارك العسكرية ٠

التكييف القانوني للجريمة

نظـــرا لعدم وجود قوانين حتى الآن في مصر خاصة بالجرائم الإلكترونية فتطبق القوانين العادية الخاصة بالجرائم القديمة التقليدية على تلك الجرائم الإلكترونية الحديـــثة و علـــيه فيمكـــن القـــول انه تطبق القواعد القانونية الخاصة بانتحال الشخصـــية علـــى تلك الجرائم المتعلقة بانتحال شخصية المواقع على أساس أن تلـــك المواقـــع لها شخصية معنوية تتساوى مع الشخصية الطبيعية التي يملكها الشخص العادي ٠

و علـــيه فـــالقواعد القانونية التي تطبق على جريمة انتحال شخصية الشخص العادة تطبق كما هي على جريمة انتحال شخصية المواقع ٠

ثانيا : جرائم الاختراق

يعتـــبر الهجوم على المواقع و اختراقها على شبكة الإنترنت من الجرائم الشائعة في العالم

وطـــبقا لمؤشـــر سام للاختراق فإن لمستويات الاختراق او الهجوم المعلوماتي ستة مستويات بحسب درجة الخطورة : –

– المستوي الأول من الهجوم ATTACK - LEVEL . 1

مـــا يعـــــرف بهجـــوم قنبلة صندوق البريد وتؤدي إلي إعاقة النظام عن تقديم الخدمــــــة .

– المستوي الثاني من الهجوم ATTACK - LEVEL . 2

الدخول غير المرخص به لنظام المعلومات أو الحاسبات بما يتيح قراءة الملفات أو نسخها للمخترق غير المرخص لـــــه .

- المستوي الثالث من الهجوم ATTACK - LEVEL . 3

يتمكن المخترق فيه من الدخل إلي مواقع غير مرخص في الدخول إليها .

- المستوي الرابع من الهجوم ATTACK - LEVEL . 4

يتمكن المخترق فيه من قراءة ملفات سرية .

- المستوي الخامس من الهجوم ATTACK - LEVEL . 5

يتمكن المخترق فيه من نقل ونسخ الملفات السرية .

- المستوي السادس من الهجوم ATTACK - LEVEL . 6

حيث يستطيع المخترق من خلال هذا المستوى من الاختراق أن يوجد قناة مفتوحة للدخول إلي سائر أرجاء النظام والعبث بمحتوياته .

هذا ويستخدم المهاجم في هجومه ما يعرف بالقنبلة المنطقية وهي برنامج يدمر البيانات أو قد يستخدم حصان طروادة وهو برنامج لاقتحام أمن النظام يتنكر في شكل برئ حتى يلج إلي النظام فيفسده .

١ - الاختراق

لكي تتم عملية الاختراق لابد من برنامج يتم تصميمه ليتيح للمخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أن يتم ذلك الاختراق و قد صمم العديد من تلك البرامج التي تتيح عملية الاختراق و تجعلها سهلة ألا أن معظم تلك البرامج كان بها نقطة ضعف أساسية تقلل كثيرا من إمكانياتها و هي إمكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه و عليه يكون من الممكن متابعة تلك البرامج و القضاء عليها فيما عدا برنامج واحد تمكن مصمموه من التغلب على هذا العيب الموجود في كافة برامج الاختراق الأخرى

و أطلق على هذا البرنامج أسـم (حصان طروادة)

و يعتـبر بـرنامج حصـان طروادة من البرامج الخطرة DANGEROUS PROGRAMS علـى الإطـلاق التـي تسـتخدم في عمليات اختراق أجهزة الحاسبات الآلية COMPUTERS نظرا لتمتعه بعدة مميزات تجعل منه الأقدر علـى عملية الاختراق دون القدرة على كشفه و تتبعـه و القضاء عليه لذلـك فقـد اكتسـب هـذا الـبرنامج شهرة كبيرة في مجال اختراق أجهزة الحاسبات الآليـة .

صـمـم برنامــج حصان طروادة في البداية بغرض حسن و مفيد هو معرفة ما يقـوم به الأبناء على جهاز الكومبيوتر COMPUTERS في غياب الوالدين أو معـرفة ما يقوم به الموظفون على جهاز الكومبيوتـر في غياب المد راء إلا انه تم تطوير هذا البرنامج بعد ذلك تطويـرا سيئا .

و تكمـن خطـورة هذا البرنامج (حصان طروادة) في كونه يتيح للمخترق أن يحصـل على كلمة سر (PASSWORDS) الدخول على الجهاز بمعنى أنه يتـيح للدخيل أن يتمكن من الدخول على الجهاز بطريقة لا تثير أي ريبة أو شك نظـرا لأنه يمكن للدخيل من الدخول على جهاز الكومبيوتر COMPUTERS باستخدام كلمة السر (PASSWORDS) التي يستخدمها صاحب الجهاز و من هنا تكمن خطورة هذا البرنامج لان الدخول على الجهاز باستخدام كلمة السر لا يمكن صاحب الجهاز من ملاحظة وجود دخيل يتمكن من الدخول على الجهاز في غيبته .

ومـن جهة أخرى فأن هذا البرنامج لا يمكن كشفه بواسطة البرامج المتخصصة فـي كشف الفيروسات و عليه فانه لا يمكن في الأغلب الأعم من الأحوال معرفة وجـود مـثل هذا البرنامج على جهاز الكومبيوتر أو الإحساس بوجوده للقضاء عليه (NANOART - 2000) .

كيفية اقتحام الجهاز

لتتم عملية التسلل لابد من زرع حصان طروادة و يتم زرعه بعدة طرق :

١ – يرسل عن طريق البريد الإلكتروني (E - MAIL) كملف ملحق حيث يقوم الشخص باستقباله و تشغيله و قد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى ٠

٢ – عند استخدام برنامج المحادثة الشهير (I C Q) و هو برنامج محادثة أنتجته إسرائيل

٣ – عند تحميل برنامج من أحد المواقع غير الموثوق بها

٤ – مجرد كتابة كوده على الجهاز نفسه

٥ – في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترنت

٦ – يمكن نقل البرنامج أيضا بواسطة استخدام برنامج (F T P) أو برنامج (TELNET)

٧ – كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص

ومن ناحية أخرى فلكي يستطيع أي برنامج اختراق أن يتم عملية الاختراق نفسها لابد من من وجود منافذ في الجهاز المراد اختراقه و من أهم تلك المنافذ التي يمكن استخدامها من قبل المتسللين و البرامج المستخدمة في النفاذ من هذه المنافذ :

2023	RIPPER
2115	BUGS
2140	DEEP THROAT . THE INVESOR

2565	STRIKER
2583	WIN CRASH
2801	PHINEAS PHUCKER
3024	WIN CRASH
3129	MASTER PARADISE
3150	DEEP THROAT . THE INVASOR
3700	PORTAL OF DOOM
4092	WIN CRASH
4567	FILE NAIL
4590	ICQ TROJAN
5000	BUBBEL . BACK DOOR SETUP . SOCKETS DE TROIE
5001	BACK DOOR SETUP . SOCKETS DE TROIE
5321	FIRE HOTCKER
5400 5401 5402	BLADE RUNNER
5555	SERVE ME
5556 5557	BO FACIL
5569	ROBO - HACK
5742	WIN CRASH
6400	THE THING
6670	DEEP THROAT
6711	SUB SEVEN
6771	DEEP THROAT
6776	BACK DOOR - G . SUB SEVEN
6939	INDOCTRINATION
6969	GATE CRASHER . PRIORITY

7300 7301 7306 7307 7308	NET MONITOR
7000	REMOTE GRAB
7789	BACK DOOR SETUP . ICKILLER
9872 9873 9874 9875 10067 10167	PORTAL OF DOOM
9989	INI - KILLER
10520	ACID SHIVERS
10607	COMA
11000	SENNA SPY
11223	PROGENIC TROJAN
12223	HACK 99 KEY LOGGER
12345	GABAN BUS NET BUS PIE BILL GARES . X - BILL
12346	GABAN BUS NET BUS . X - BILL
12361 12363	WHACK - A - MOLE
12631	WHCK JOP
13000	SENNA SPY
16969	PRIORITY
20001	MILLENNIUM
20034	NET BUS 2 PRO
21544	GIRL FRIEND
22222	PROSIAK

23456	EVIL FTP . UGLY FTP
26274	UPT - DELTA SOURCE
29891	UPT - THE UNEXPLAINED
30029	AOL TROJAN
30100 30101 30102	NET SPHERE
30303	SOCKETS DE TROIE
31337	BAROON NIGHT . BO CLIENT . BO 2 . BO FACIL UPD - BACK FIRE . BACK ORIFICE . DEPP BO
31338 31339	NET SPY DK
31338	UPD - BACK ORIFIC . DEEP BO
31666	BO WHACK
33333	PROSIAK
34324	BIG GLUCK . TN
40412	THE SPY
40421	AGENT 40421 . MASTER PARADISE
40422 40423 40426	MASTER PARADISE
47262	UPD - DELTA SOURCE
50505	SOCKETS DE TROIE
50766	FORE
53001	REMOTE WINDOWS SHUTDOWN
54321	SCHOOL BUS
60000	DEEP THROAT
61466	TELECOMMANDO
65000	DEVIL

المصدر : موقـــع

HTTP://WWW.NANOART.F2S.COM/HACK/PORTS3.HTM

و المـــنافذ تلك يمكـــن وصفـــها ببوابات الجهاز و هناك ما يقرب من ٦٥٠٠٠ (خمســـة و ستون ألف) منفذ تقريبا في كل جهاز و يميـــز كل منفذ عن الآخر بـــرقـــــم خـــاص بـــــه و لكــل منفذ غرض محدد فمثلا المنفذ رقـــم ٨٠٨٠ يخصـــص أحـــيانا لمزود الخدمة و هذه المنافذ غير مادية مثل منفذ الطابعة و تعتـــبر جـــزء مـــن الذاكـــرة لها عنوان معين يتعرف عليها الجهاز أحيانا بأنها مـــنطقـــة إرسال و استقبال البيانات و كل ما يقوم بـــه المتسلل هـــو فتح أحد هـــذه المـــنافذ للوصـــول إلى جهاز الضحية وهو ما يعرف بطريقة الزبـــون / الخـــادم (CLIENT / SERVER) حيث يتم إرسال ملف لجهاز الضحية ليقوم يفتح تلك المنافذ فيصبح جهاز الضحية (SERVER) و جهاز المتسلل (CLIENT) و مـــن ثـــم يقـــوم المتسلل بالوصول إلى تلك المنافذ باستخدام برامج كثيرة متخصصة كبرنامج (NET BUS) أو (NET SPHERE) و لعـل الخطـــورة الإضـــافيـــة تكمـــن في انه عند دخول المتسلل إلى جهاز الضـــحية فانه لن يكـــون الشخص الوحيد الذي يستطيع الدخول إلى ذلك الجهاز حيـــث يصـــبح ذلـــك الجهاز مركزا عاما يمكن لأي شخص الدخول عليه بمجرد قـــيامه بعمـــل مســـــــح للمنافذ (PORTSCANNING) عن طريق أحد البرامج المتخصصة في ذلك ٠

وقـــد كـــثرت حالات الاختراق عبر شبكة الإنترنت و كونها لم تعد تقتصر على المحترفين فقط بل أصبحت عمليات الاختراق يقوم بها بعض الهواة و تكون في قوتها وكأن محترفين شديدي الاحتراف هم القائمين بها ٠

فقـــد تعرضت مثلا مواقع وزارت العدل و المخابرات المركزية و القوات الجوية الأمريكييـــن إلـــى الاقـــتحام و الاختراق كما تعرض له أيضا موقع حزب العمل الإنجليزي ٠

وفي عام ١٩٩٧ م قدرت وكالة المباحث الفيدرالية الأمريكية و يرمز لها بـــ (F B I) تعــرض حوالـــي ٤٣ % من الشركات التي تستخدم خدمة الإنترنت لمحاولات اختراق تتراوح بيم (٣ – ٥) مرات خلال سنة واحدة . (WILSON – 2000) .

و محـــاولات الاختراق و الاقتحام لا يقوم بها المحترفون فقط و إنما قد يقوم بها الهـــواة أيضـــا من باب إثبات الذات و القدرة على القيام بتلك المحاولات بنجاح مـــثلهم فـــي ذلك مثل المحترفين و مثال ذلك ما حدث مع مراهقة في الخامسة عشـــر من عمرها عندما قامت بمحاولة اختراق إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة و كان تبريرها لما قامت به أنها قـــد ملت من مشاهدة التليفزيون ففكرت في شئ آخر تقوم به يبدد ما تشعر به من ملل (KOERNER - 1999) .

ومـــرة أخرى أثناء حرب الخليج الأولى عندما اتضح لوكالة المباحث الفيدرالية الأمريكـــية (F B I) عـــندما اجروا تحقيقا حول تسلل أشخاص إلى الصفحة العنكبوتـــية الخاصـــة بـــإحدى القواعد العسكرية الأمريكية و كانت الشكوك في الـــبداية تـــتجه إلى أن التسلل قد حدث من إرهابيين دوليين محترفين ألا انه قد اتضـــح فـــي الـــنهاية أن المتســـلل ما هو ألا مراهقان تسللا عن طريق جهاز الكومبيوتر من منزلهما (WILSON – 2000) .

و فـــي عام ١٩٩٧ م قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية فـــي مطـــار (MASSACHUSETTS) مما أدى إلى تعطيل نظام الملاحة الجويـــة لمـــدة ســـتة ساعات و بالرغم من فداحة الضرر الذي تسبب فيه هذا التســـلل ألا أن عقوبـــة المـــراهق الذي قام بالتسلل اقتصرت على وضعه نحن المراقبة لمدة سنتين فقط (WILSON - 2000) .

و هنا نجد أمرا هاما يعمل على كثرة عدد من يحاولون اختراق أجهزة الحاسبات الآلـية الخاصـة بالمطـارات و القواعد العسكرية و البنوك و ما إلى ذلك من عملـيات الاخـتراق التـي تتم لعدد كبير من أجهزة الحاسبات الآلية الخاصة بمناطق و أماكن حساسة لا تتحمل ذلك العبث بأجهزتها ٠

أن عــدم وجـود العقوبة القانونية الشديدة التي تجعل من يريد القيام بعملية اخـتراق يفكـر ألف مرة و مرة قبل القيام بتلك المحاولة هو العامل الأهم في زيـادة تلـك العمليات و عدم قدرة الأجهزة الأمنية على محاولة الحد منها لان القـانون لا يساعدها على القيام بالواجبات المنوط بها القيام بها و يبقى أمامها شـئ واحـد فقط يعد هو سبيلها الوحيد لمحاولة وقف هذا السيل من محاولات الاخـتراق ألا وهـو محاولـة الوقـوف أمـام هؤلاء المتسللين بمحاولة القيام بإجـراءات إلكترونـية مـتقدمة و شديدة التعقيد في محاولة منهم لجعل القيام بمحاولـة تسـلل هي من الأمور الصعبة جدا و التي لا يستطيع حتى المحترفين القيام بها ٠

و قـد أوضحت دراسة أجريت عام ١٩٧٩ م على عـدد (٥٨١) طالب جامعي أمريكي أن نسبة ٥٠ % منهم قد اشترك في أعمال غير نظاميـة أثناء استخدام الإنترنـت خلال ذلك العام و أن (٤٧) طالـب أو ما نسبته ٧,٣ % سبق وان قبض عليه في جرائم تتعلق بالحاسب الآلـي وان ٧٥ طالبا منهـم أو ما نسبته ١٣,٣ % مـنهم قبض على أصدقائهم في جرائم تتعلـق أيضا بالحاسـب الآلي (SKINNER & FREAM . 1997)

ومن المعروف أن عدد جرائم من تلك النوعية قد تضاعفت في الولايات المتحدة الأمريكية ففى عام ١٩٩٩ م تحرت وكالة المباحث الفيدرالية (F B I) عن (٨٠٠) حالة تتعلق بالتسلل (HACKING) وهو ضعف عدد الحوادث التي

قامت بالتحرى عنها في العام السابق أي عام ١٩٩٨ م أما الهجوم على شبكات الحاسب الآلي على الإنترنت فقد تضاعف هو الآخر ألا أن نسبة الزيادة قد بلغت (٣٠٠ %) في ذلك العام أيضا وهى زيادة رهيبة ٠

و في محاولة من قيام الجهات الأمنية المسئولين عن أمن الحاسبات الآلية ببناء هذا الجدار الأمني الإلكتروني و بمساعدة تقنية و فنية من المتسللين أنفسهم بل و المحترفين منهم على وجه الخصوص ٠

فعلى سبيل المثال يرسل مسئولي أمن الحاسبات الكثير من الأسئلة التي تتعلق بأحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف بأسم (HACKER INTERNET CHAT ROOM) و لطلب نصائح تقنية حول احدث سبل الحماية ٠

بل أن الأكثر من ذلك أن وكالة المباحث الأمريكية (F.B.I) استعانت أيضا بخبراء في التسلل (HACKERS) لتدريب منسوبى الوكالة على طرق التسلل (HACKING) لتنمية خبراتهم و قدراتهم في هذا المجال و ليستطيعوا مواكبة خبرات و قدرات المتخصصين و المحترفين من المتسللين (HACKERS) ومنهم أحد اشهر المتسللين في العالم و يدعى (BRIAN MARTIN) و هو مشهور بأسم (JERICHO) وهم متهم حاليا بتهمة التسلل و العبث بمحتويات الصفحة الرئيسية لصحيفة (NEW YOURK TIMES) على شبكة الإنترنت (STAFF . 2000 . APRIL 2) ٠

وقد أكدت وحدة الخدمات السرية الأمريكية (THE U S SECRET SERVICE) أن الجرائم المنظمة قد بدأت في الاتجاه نحو استغلال التسلل (HACKING) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية (THOMMAS . 2000) ٠

وفـــى خبر نشرته صحيفة (لوس أنجلوس تايمز) أوضح أن متسللين قاموا باقـــتحام نظـــام الحاســـب الآلي الذي يتحكم في تدفق اغلب الكهرباء في ولاية كاليفورنيا الأمريكية ٠

حذرت مصادر أمنية من ظهور تقنية جديدة تتيح للمخربين اختراق اكثر الأجهزة الحاســوبية حصـــانة عــن طريق تطوير جيل جديد من الملفات التجسسية التي بإمكانهـــا الـــتحايل علـــى أنظمـــة الحماية المثبتة في نسبة كبيرة من الأجهزة الشخصية المرتبطة بالإنترنت.

وصدر التحذير من جماعة أمنية ونشر موقع **WWW.PCWORLD.COM** أجزاء منه وتضمن معلومات غاية في الخطورة تشير إلى قيام ألها كرز بتطوير تقنـــية جديـــدة تمكـــن أحصنة طروادة أو الملفات التجسسية **TROJAN** من اقـــتحام الأجهـــزة الشخصية حتى في ظل برامج وجود حماية كبرامج الجدران الـــنارية **FIER WALL** عن طريق الاستفادة من ثغرات أمنية معروفة في متصفح الإنترنت - إنترنت اكسبلورر - في إصدارته العديدة.

وقال التقرير أن الفكرة التي تم تطويرها باستخدام تقنيات تخريبية متقدمة تتمثل فـــي قـــيام الملـــف التجسســـي بفتح ثغرة في متصفح الإنترنت وتسخيرها لأي مخترق يمتلك البرامج الخاصة بذلك لتمكنه من العمل خفية في الجهاز المصاب حـــتى في ظل وجود برامج الجدرأن النارية **FIER WALL** التي لن تتعرف عليه مشيرا إلى انه يمكنه استخدام ملقم خارجي لا يمكن للجدار الناري تحديده فـــي حالـــة تـــم القيام بمسح الجهاز المصاب لأنه يعمل باستخدام ملقمات تتيح إخفاء هوية مستخدميها.

و أضاف التقرير أن التقنية الجديدة ستتيح للها كرز اختراق أي جهاز حتى ولو كان يتضمن جدارا ناريا قويا مشيرا إلى أن التقنية تمثل نجاحا لجهود ألها كرز الذين قاموا بتطوير المزيد من البرامـــج التي تتجاوز إمكانات جدرأن الحماية

الـــنارية والتي تقوم في الغالب بصد هجماتهم ودعا التقرير شركة مايكروسوفت إلـــى قـــيامها بســـد الـــثغرات الأمنـــية في متصفحتها الحالية والسابقة مطالبا المستخدمين أنفسهم بالقيام بنفس المهمة لتحصين متصفحاتهم التي تعد بمثابة جواز السفر في العالم الافتراضي.

٢ – الإغراق بالرسائل

لـــم تـــتوقـــف محاولات المتسللين عن التوصل إلى طـــرق جديدة يمكنهم من خلالهـــا العمل على الأضرار بأجهزة الحاسبات الآلية COMPUTERS دونما أي اســـتفادة ألا إثـــبات تفوقهـــم في ذلك ومن تلـــك الطرق التي توصلوا إليها طـــريقة الإغراق بالبريد الإلكتروني و تلك الطريقة تعني إرسال كـــم هائـــل من الرســـائل SENDING A LOT OF MESSAGES عـــبـــر الـــبريد الإلكترونـــي E _ MAIL لأجهـــزة الحاســـبات الآليـــة COMPUTERS المـــراد العمـــل علـــى تعطيلها و وتوقفها عن العمل و بالفعل فأن تلك الرسائل الكثيرة والتى لا تعنى شئ على الإطلاق ٠

فـــتلـــك الرســـائل MESSAGES قـــد تكون محملة بملفات FILES كبيرة الحجـــم لمجـــرد التأثـــير علـــى الجهـــاز نظرا لصغر المساحة المحددة للبريد الإلكترونـــي E _ MAIL في معظم الأحيان – و التي تصل لجهاز الحاســـب الآلـــي COMPUTERS مـــرة واحـــدة و في وقت واحد تقريبا تعمل على توقفـــه عـــن العمـــل علـــى الفـــور نظرا لما تسببه من ملء منافذ الاتصال (COMMUNICATION - PORTS) و كذلـــك مـــلء قوائم الانتظار (QUEUES) و بمجـــرد توقـــف تلك الأجهزة COMPUTERS عن العمل تنقطع بالتالي الخدمة التي تؤديها تلك الأجهزة ٠

٣ - الفيروسات VIRUSES

الفــيروس هــو برنامج مثل أي برنامج آخر موجودا على جهاز الحاسب الآلي VIRUSES IS A PROGRAM LIKE ANY ANOTHER PROGRAM ON THE COMPUTER و لكــنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على جهاز الحاسب الآلي سواء بأن تجعــل تلــك الــبرامج الأخرى نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى من على جهاز الحاسب الآلي و بالتالي تعطلها عن العمل .

و أمــا عــن بدأ عملها فبدأ عملها يتحدد طبقا لأسلوب تصميمها فقد تبدأ تلك الفيروســات العمل بمجرد فتح الرسالة الموجودة بها و التي وصلت عن طريق الــبريد الإلكترونــي و قد تبدأ العمل بمجرد تشغيل البرنامج الموجودة عليه في الجهاز و هكذا .

سبب التسمية

ســمي الفــيروس (VIRUS) بهــذا الاســم لتشــابه آلــية عمله مع تلك الفيروســات التــي تصيب الكائنات الحية بعدد من الخصائص كخاصية الانتقال بــالعدى و كونه كائنا غريبا يقوم بتغيير حالة الكائن المصاب إضافة إلى الضرر الذي يتسبب فيه أن يتم العلاج بإزالته .

أنواع الفيروسات

TYPES OF VIRUS

و يمكننا تقسيم تلك الفيروسات إلى أنواع هي :

- النوع الأول

فيروسات الجزء التشغيلي للاسطوانة كفيروس (BRAIN) و (NEWZELAND)

- النوع الثاني

الفيروسات المتطفلة كفيروس (CASCADE) و (VIENNA)

- النوع الثالث

الفيروسات المتعددة الأنواع كفيروس (SPANISH - TELECOM) و (FLIP)

- النوع الرابع

الفيروسات المصاحبة للبرامج التشغيلية (EXE) سواء على نظام الدوس أو نظام الويندوز

و يمكن تقسيم الفيروسات على أساس آخر وهو المكان المستهدف بالإصابة داخل جهاز الكومبيوتر و على هذا الأساس يتم تقسيم الفيروسات إلى ثلاثة أنواع هي :

النوع الأول : فيروسات قطاع الإقلاع (BOOT SECTOR)

النوع الثاني : فيروسات الملفات (FILE INJECTORS)

النوع الثالث : فيروسات الماكرو (MACRO VIRUS)

و هناك تقسيم ثالث يمكن تقسيم الفيروسات إليه ولكن في هذا التقسيم يتم تقسيم الفيروسات إلى

١ – فيروسات الإصابة المباشرة

٢ – الفيروسات المقيمة

٣ - الفيروسات المتغيرة

١ - فيروسات الإصابة المباشرة DIRECT ACTION

و هي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها

٢ - الفيروسات المقيمة STAYING

و هي التي تظل كامنة في ذاكرة الجهاز و تنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما و معظم الفيروسات تندرج تحت هذا النوع

٣ - الفيروسات المتغيرة POLYMORPHS

و هي الفيروسات التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات التي قد تستخدم للقضاء عليها

و من جرائم إرسال فيروسات قيام شخص أمريكي يدعى (ROBERT MORRIS) بإرسال دودة حاسوبية بتاريخ ٢ / ٨ / ١٩٨٨ م عبر الإنترنت و قد كرر الفيروس (VIRUS) نفسه عبر الشبكة بسرعة فائقة فاقت حتى تصور مصمموها نفسه و قد أدى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) حاسب إلى مرتبط بالإنترنت و قد قدرت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات و لو قدر لمصمم الفيروس أن يصممه ليكون اشد ضررا لكان قد لحقت أضرارا أخرى لا يمكن حصرها بتلك الأجهزة و قد حكم عليه بالسجن ثلاث سنوات بالرغم من انه دافع عن نفسه بأنه لم يكن يقصد إحداث كل هذا الضرر ٠

المصدر : موقع

HTTP://WWW.MINSHAWI.COM/INTERNETCRIM

كيفية اقتحام الجهاز

لتتم عملية التسلل لابد من زرع حصان طروادة و يتم زرعه بعدة طرق :

١ – يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص باستقباله و تشغيله و قد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى ٠

٢ – عند استخدام برنامج المحادثة الشهير (I C Q) و هو برنامج محادثة أنتجته إسرائيل

٣ – عند تحميل برنامج من أحد المواقع غير الموثوق بها

٤ – مجرد كتابة كوده على الجهاز نفسه

٥ – في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترنت

٦ – يمكن نقل البرنامج أيضا بواسطة برنامج (F T P) أو (TELNET)

٧ – كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص

الديدان WORMS

تعريفها DEFINITION

هي برامج صغيرة قائمة بذاتها و غير معتمد على غيرها و صنعت للقيام بأعمال تدميرية أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم على شبكة الإنترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم و تلك الديدان تتميز بسرعة الانتشار و في نفس الوقت يصعب التخلص منها نظرا لقدرتها الفائقة على التلون و التناسخ و المراوغة ٠

آلية عمل الديدان

تختلف الديدان في طريقة عملها من نوع إلى آخر فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة بينما بعضها يتخصص في البريد الإلكتروني بحيث تقوم بإرسال نفسها في رسائل إلى جميع من توجد عناوينهم في دفتر العناوين الموجود بالجهاز و أنواع أخرى من الديدان تقوم بإرسال رسائل قذرة إلى بعض الموجودة عناوينهم في دفتر العناوين الموجود بالجهاز بأسم مالك البريد مما يوقعه في حرج بالغ مع من تم إرسال تلك الرسائل إليهم

و تكمن خطورة الديدان في استقلاليتها و عدم اعتمادها على أي برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع و مما لا شك فيه انه توجد أنواع منها في غاية الخطورة حتى أن بعضها اصبح كابوسا مرعبا كل ملازم للشبكة و مثال ذلك تلك الدودة التي ظهرت في أكتوبر عام ٢٠٠٢ م و اشتهرت بأسم (TANATOS) و انتشرت انتشار النار بالهشيم و خلفت ورائها آثارا تدميرية هائلة .

من المعلوم أن اشهر وسائل انتشار الديدان هو عن طريق الرسائل الإلكترونية المفخخة و التي عادة ما تكون عناوين تلك الرسائل جذابة كدعوة لمشاهدة صور أحد النجوم أو المشاهير لذلك لابد من توخي الحذر حتى وان كانت تلك الرسائل من مصدر معروف و موثوق به لان تلك الديدان تقوم بإرسال نفسها في شكل رسائل إلى كافة الموجودة عناوينهم على الجهاز

كيفية الحماية من الديدان

تتم الحماية من الديدان بتركيب أحد البرامج المضادة للديدان و المتخصصة في ذلك (WORM GUARD) أو بتركيب أحد البرامج المضادة للفيروسات بصفة عامة .

التكييف القانوني للجريمة

تعد جريمة التسلل أو الاختراق لأجهزة الحاسبات الآلية الخاصة بالغير هي جريمة تنطبق عليها النصوص القانونية المتعلقة بالدخول إلى ملك الغير و العبث بما به من محتويات أو تخريبها أما إذا زاد على ذلك سرقة بعض تلك المحتويات فتزاد هنا جريمة السرقة .

فتنص المادة ٣٦٩ من قانون العقوبات المصري على أن ((كل من دخل عقارا في حيازة آخر بقصد منع حيازته بالقوة أو بقصد ارتكاب جريمة فيه .... يعاقب بالحبس مدة لا تجاوز سنة أو بغرامة لا تجاوز ثلاثمائة جنيه مصري))

كما تنص المادة ٣٦١ من قانون العقوبات المصري على انه ((كل من اتلف عمدا أموالا ثابتة أو منقولا لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأي طريقة يعاقب بالحبس مدة لا تزيد على ستة اشهر أو بغرامة لا تجاوز ثلاثمائة جنيه مصري لا غير .

فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيها فأكثر كانت العقوبة الحبس لمدة لا تجاوز سنتين و غرامة لا تجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين .

و تكون العقوبة مدة لا تزيد عن خمس سنوات و لا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة أو إذا ترتب عليه جعل حياة الناس أو أمنهم في خطر .

و يضاعف الحد الأقصى للعقوبة إذا ارتكبت الجريمة تنفيذا لغرض إرهابي))

و عليه و على اعتبار أن جهاز الحاسب الآلي هو عقار يحتفظ فيه الناس بكافة أو على الأقل بمعظم متعلقا تهم المعلوماتية الهامة بل و الكثير من أسرارهم المعلوماتية الخاصة بما يملكونه من أموال أو معلومات فهو يسرى عليه ما تم

النص عليه في المادة ٣٦٩ من قانون العقوبات المصري ٠
و أيضـا يعـد جهـاز الكومبيوتر هو أموال منقولة فالتسلل إليها و تخريبها أو تعطيلها عن العمل يسرى عليها المادة ٣٦١ من قانون العقوبات المصري ٠

ثالثا : الجرائم المالية

تنقسم الجرائم المالية التي تتم عبر الإنترنت إلى ستة أنواع من الجرائم هي :

- ١ – جرائم السطو على أرقام البطاقات الائتمانية
- ٢ – لعب القمار
- ٣ – تزوير البيانات
- ٤ – الجرائم المنظمة
- ٥ – تجارة المخدرات
- ٦ – غسيل الأموال

١ – جرائم السطو على أرقام البطاقات الائتمانية

مـنذ أن بدأ استخدام البطاقات الائتمانية عبر شبكة الإنترنت حتى كان اللصوص المتسـللين فـي أعقابها بلا هوادة فالبطاقات الائتمانية تعد نقودا إلكترونية و الاستيلاء عليها يعد استيلاء على مال الغير ٠
و نظرا لسهولة الاستيلاء على تلك الأرقام فقد تزايدت حوادث الاستيلاء عليها و أيضـا تزايدت عمليات الابتزاز المصاحبة لارتكاب مثل تلك الجرائم و عمليات الابـتزاز تلك تكون أما لإعادة تلك الأرقام أو لعدم نشرها أو لعدم استخدامها من قبل من استولى عليها ٠

و قـد وقعـت بـالفعل عـدة حوادث من ذلك النوع و منها قيام شخص ألماني بالدخول غير المشروع إلى أحد مزودي الخدمة و استيلاءه على أرقام البطاقات الائتمانية الخاصة بالمشتركين و من ثم بدأ في ابتزاز صاحب الخدمة بنشر تلك الأرقـام أو سداد فدية مالية ألا أن الشرطة الألمانية قد نجحت في القبض على ذلك اللص المتسلل عند استلامه الفدية ٠

كمـا قام شخصان في عام ١٩٩٤ م بإنشاء موقع على شبكة الإنترنت مخصص لشـراء طلـبات يـتم إرسالها بمجرد سداد قيمتها إلكترونيا ألا انه كان الغرض الأساسـي مـن إنشـاء هذا الموقع هو الاستيلاء على أرقام البطاقات الائتمانية الخاصة بالمشترين من هذا الموقع أي أن الغرض الأساسي من هذا الموقع كان النصـب و الاحتـيال على مرتاديه للحصول منهم طواعية على أرقام بطاقاتهم الائتمانية

و قـد اثبتـت شـبكة (MSNBC) عمليا مدى سهولة الحصول على أرقام الـبطاقات الائتمانـية من شبكة الإنترنت حيث قامت بعرض قوائم تحتوى على اكـثر مـن ٢٥٠٠ رقـم بطاقة ائتمانية حصلت عليها من سبع مواقع للتجارة الإلكترونـية و ذلك عن طريق استخدام قواعد بيانات متوافرة تجاريا و لم يكن ممن الصعب على أي متطفل أو متسلل استخدام تلك الوسيلة البدائية الوصول و الاسـتيلاء علـى تلـك الارقام و استخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون ٠

و يـتعدى الأمر المخاطر الأمنية التي يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن في بداية ثورة نقدية يطلق عليها أسـم النقود الإلكترونية (ELECTRINIC CACH) أو (CYBER CACH) و التـي يتنبأ لها بأن تكون مكملة للنقود الورقية أو البلاستيكية (بطاقات الائتمان) و

من المتوقع أيضا أن يزداد الاعتماد على هـذا النـوع الجديـد و الحديث مـن النقـود (CACH) و أن تحوز الثقة (CONFIDENCE) التي تحوزها النقود التقليدية هذا بجانب الأسهم و السندات الإلكترونية المعمول بها حاليا في دول الاتحـاد الأوروبي حاليا و التي اقر الكونجرس الأمريكي العمل و التعامل بها عام ١٩٩٠ م ٠

فـإذا كانـت الـبطاقات الائتمانية الحالية تواجه كل تلك المخاطر فما الحال عند استخدام الأنواع الجديدة من النقود الإلكترونية (ELECTRINIC CACH) فنحـن بحاجة إلى تدعيم الثقة في تلك الأنواع من النقود التي يتم استخدامها حالـيا عبر شبكة الإنترنت حتى تجد الأنواع الجديدة من النقود الإلكترونية الثقة اللازمـة ليتعامل بها الأفراد دون خوف من اعتداء اللصوص المتسللين إليها و إفشاء بياناتها و سرقتها ٠

التكييف القانوني للجريمة

سرقة أرقام البطاقات الائتمانية تعد جريمة موازية تماما لجريمة سرقة النقود و هـي جـريمة منصوص عليها في كافة القوانين فجريمة السرقة هي جريمة تعد مـن اقـدم الجـرائم المعروفة على مستوى العالم و عليه فهي منصوص على تجريمها في كافة قوانين العالم ٠

وفي مصر تنص المادة ٣١١ من قانون العقوبات المصري على أن

((كل من اختلس منقولا مملوك للغير فهو سارق))

و تخـتلف العقوبـة المقررة على جريمة السرقة بحسب وجود أي من العوامل المشددة للجريمة كوجود سلاح مع السارق أو أن تتم تلك السرقة في الليل و ما إلى ذلك من العوامل التي تعد عوامل مشددة للعقوبة ٠

و رغـم أن تلـك العوامل ليس لها محل في جريمة سرقة أرقام بطاقات الائتمان عن طريق الإنترنت إلا أن جريمة السرقة كجريمة معاقب عليها .

٢ – ممارسة القمار

في الماضي كان لعب القمار يستلزم وجود اللاعبين معا على طاولة ليتمكنوا من لعـب القمـار معا أما الآن و مع انتشار شبكة الإنترنت على مستوى العالم فقد اصـبح لعب القمار اسهل و اصبح تجمع اللاعبين على مستوى العالم في مكان واحـد اسـهل من ذي قبل على الإطلاق فقد اصبح بإمكان اللاعبين التجمع معا عبر شبكة الإنترنت و لعب جميع أنواع القمار من خلال الشبكة .
كمـا أن انتشار المواقع على شبكة الإنترنت التي توفر لمثل هؤلاء اللاعبين ما يحـتاجونه من برامج ليتمكنوا من لعب القمار قد ذادت و انتشرت على الشبكة نظرا لان اللاعبين بات بإمكانهم اللعب و كل منهم في منزله دون أن يضطر إلى مجرد الخروج من منزله و الذهاب إلي الأماكن التي يمكنه اللعب فيها .
و عليه فأن انتشار شبكة الإنترنت قد اسهم من ضمن ما اسهم فيه من السلبيات انتشار لعب القمار .
و نظرا لان القمار قد يكون مصرحا به في بعض البلاد إلا انه الأغلب الأعم من الـبلاد مصـرح به و لكن بشكل محدود جدا و في بعض الأماكن السياحية فقط دون أن يكـون مصـرحا به في الأماكن العادية التي يرتادها الأغلب الأعم من أفـراد الشعب نظرا لأنه يخالف تعاليم الدين في كافة البلاد العربية التي يرفض الدين الإسلامية لعب القمار و يحرمه .
و بالتالي فلعب القمار غير مصرح به حتى ولو كان عن طريق الإنترنت .
و حتى في أمريكا فان لعب القمار عبـر شبكة الإنترنت غير مصرح به قانونا

علـــى الإطـــلاق و ليـــتفادى أصحاب المواقع تلك المشكلة القانونية يلجأون إلي إدارة تلك المواقع المشبوهة من خارج حدود الولايات المتحدة الأمريكية .

ولذلـــك فقـــد بدأت الأصوات تعلوا هناك من اجل البدء في ملاحقة القائمين على تلك المواقع لمخالفتهم القانون الذي يجرم لعب القمار عبر الشبكة إلا أن الأرباح الخيالـــية التـــي يجنيها أصحاب تلك المواقع تدفعهم إلي المراوغة و الهرب من تلـــك الملاحقـــة حـــتى لا يغلقوا تلك المواقع التي يربحون من ورائها مليارات الـــدولارات من اللاعبين الذين يدخلون على مواقعهم من كافة دول العالم دونما خوف من مخالفة القانون في بلادهم .

التكييف القانوني للجريمة

لعـــب القمـــار – بكافـــة أنواعه – هو من الأمور المعاقب عليها في معظم بلاد العـــالم و كافة البلاد الإسلامية إلا انه قد يكون مصرحا به فقد في بعض الأماكن السياحية فقط و كعامل من العوامل التي تعمل على تنشيط السياحة .

و عـــدم قانونية لعب القمار تسرى على كافة أنواع لعبه سواء بطريقة مباشرة كالطرق المباشرة و الطرق غير المباشرة كلعبه عن طريق الإنترنت .

و في مصر تنص المادة ٢٥٢ من قانون العقوبات على انه ((كل من اعد مكانا لألعـــاب القمـــار و هيأه لدخول الناس فيه يعاقب هو و صيارف المحل المذكور بالحـــبس و بغـــرامة لا تجـــاوز ألف جنيه و تضبط جميع النقود و الأمتعة في المحلات الجارى فيها الألعاب المذكورة و يحكم بمصادرتها))

و يســـرى هـــذا النص على كل من انشأ موقعا على الإنترنت للعب القمار طالما كـــان منشأ هذا الموقع مصري أو غير مصري طالما أنشأه من مصر كما يسرى هـــذا الـــنص أيضـــا علـــى كـــل من دخل على هذا الموقع للعب القمار فيما لو استطاعت السلطات التوصل إليه .

٣ – تزوير البيانات FORGERY OF DATA

تعتبر جرائم تزوير البيانات من اكثر الجرائم شيوعا من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الإنترنت أو ضمن جرائم الحاسب الآلي نظرا لأنه لا تخلوا جريمة من الجرائم إلا و يكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بآخر ٠

و تزويـــر البـــيانات FORGERY OF DATA يكـــون بـــالدخول – سواء بطـــريقة شـــرعية أو غـــير شـــرعية – على قاعدة البيانات DATABASE الموجـــودة و تعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل ٠

و مـــن تلـــك الحوادث التي تم فيها الدخول على قاعدة البيانات DATABASE بطـــريقة شـــرعية تلك الحادثة التي وقعت في ولاية كاليفورنيا الأمريكية حيث عمـــدت مدخلـــة البيانات بنادي السيارات و بناء على اتفاق ملسبق بينها و بين صـــديقها – لـــص سيارات – بتزوير البيانات FORGERY OF DATA الخاصة بملكية السيارات و المسجلة في الحاسب الإلكتروني بحيث تصبح بأسم صـــديق الفـــتاة و هو أحد لصوص السيارات و الذي يعمد إلى سرقة السيارة و بيعها و بالتالي عندما يتقدم مالك السيارة الحقيقي للإبلاغ عن سرقة سيارته و بالبحـــث في قاعدة البيانات DATABASE بالحاسب الإلكتروني يتضح عدم وجـــود ســـجلات للسيارة باسمه و بعد أن يقوم صديق الفتاة ببيع السيارة تقوم ذات الفـــتاة بإعادة تسجيل السيارة بأسم صاحبها الأصلي أي إعادة البيانات كما كانت عليه دون أي تعديل و قد كانت تلك الفتاة تتقاضى عن كل عملية من تلك العملـــيات مـــبلغ مائـــة دولار لا غـــير و قد استمرت في عملها هذا إلى أن تم اكتشافها و القبض عليهـــا ٠

تلـــك الجـــريمة هـــي مـــثال واضـــح و صـــريح علـــى جرائم تزوير البيانات FORGERY OF DATA و مـــا تسببه من ضياع الحقوق و زيادة جرائم الســـرقة التـــي تـــتزايد بنســـب كبيرة بعد استخدام عمليات تزوير البيانات في تسهيلها فعمليات تزوير البيانات يكون الغرض الأساسي منها في معظم الأحيان هو تسهيل عمليات السرقة التي لا يمكن إتمامها إلا بتزوير البيانات ٠

وفـــي حادثـــة أخرى قام مرتكبها بالدخول على قاعدة البيانات DATABASE بطـــريقة شرعية أيضا حيث قام مشرف تشغيل الحاسب بأحـــد البنوك الأمريكية أيضـــا بعملـــية قـــام مـــن خلالها بتزوير بيانات FORGERY OF DATA حســـابات أصدقائه في البنـــك بحيث تزيد أرصدتهم عما هي عليه و من ثم يتم ســـحب تلـــك الأرصدة من قبـــل أصدقائـــه بعد زيادتها و قد نجح في ذلك عدة مـــرات و قـــام أصـــدقائه بســـحب الكثير من الأموال و كان هذا الشخص ينوى الـــتوقف قـــبل موعـــد المراجعة الدورية لحسابات البنـــك إلا أن طمع أصدقائه اجـــبره علـــى الاستمرار في ارتكاب تلـــك العمليات الإجرامية إلى أن تم القبض عليـــه ٠

هـــذا مـــن جهة و من جهة أخرى فأن اتجاه الحكومات على مستوى العالم إلى الاتجاه إلى الحكومات الإلكترونية ELECTRONIC GOVERNMENT و كذلـــك انتشار التجارة الإلكترونية ELECTRONIC COMMERCE عـــبر دول العـــالم وصـــدور القوانين المنظمة له سيزيد من فرص ارتكاب تلك الجـــرائم CRIMES و فـــي نفس الوقت سيعمل على إضعاف فرصة القبض علـــى مرتكبـــي تلك الجرائم فالحكومات الإلكترونية هي المناخ الأنسب لارتكاب مثل تلك الجرائم ٠

فالارتـــباط الذي سيتم فيما بين البنوك و الشركات و الحكومات بشبكة الإنترنت ستعمل على تهيئة المناخ اكثر و اكثر لتنفيذ مثل تلك الجرائم ٠

التكييف القانوني للجريمة

جـريمة الـتزوير هـي الأخرى من الجرائم المنصوص على تجريمها في كافة القوانين ولا توجد أي دولة لا تجرم قوانينها عمليات التزوير .
فجريمة التزوير لا توجد دولة لا تجرمها بل ولا تشدد في العقوبات المقررة على ارتكابها .
وفـي مصـر فقـد افرد المشرع المصري الباب السادس عشر كاملا في قانون العقوبـات للـنص على تجريم عمليات التزوير أيا كان مرتكبها و سواء ارتكبت علـى توقيع أو بيان أو خلافه و قد نص المشرع المصري على تجريمها بداية من المادة ٢٠٦ و حتى المادة ٢٢٧ .

رابعا : الجرائم المنظمة

عصـابات المافـيا هم اشهر من قام بالجرائم المنظمة فعلى الرغم من أن هناك الكثير من العصابات على مستوى العالم تقوم بالجرائم المنظمة ذات الخبيرة في التنفـيذ و الخطـيرة التأثـير إلا أن عصـابات المافيا هي الأشهر من بين تلك العصابات .
و شـبكة الإنترنـت كانت من أهم الوسائل التي ساعدت كثيرا أعضاء عصابات المافـيا على تطوير و تحسين عملياتهم على مستوى العالم إذ أنها عملت على إلغاء حاجز الزمان و المكان من أمامهم فأصبحت عملياتهم اكثر تطورا و اعظم تأثيرا على مستوى العالم حتى أن تلك العصابات قد أقامت لها مواقع على شبكة الإنترنت لتتفادى القوانين ففي بلد ما قد يمنع القانون فعل ما بينما في بلد آخر قد لا يمنع القانون بها نفس الفعل .

ان القــدرات والفــرص التي تؤمنها شبكة الإنترنت طورت العديد من النشاطات الــتجاريــة المشــروعة مــن خــلال زيــادة سرعة وسهولة ومجالات إجراء المعــاملات إضافة الى تخفيض الكثير من النفقات واكتشف المجرمون أيضاً أن شــبكة الإنترنــت تستطيع أن تؤمن فرصاً جديدة وفوائد متضاعفة للأعمال غير المشــروعة فالجانب المظلم من الإنترنت لا يشمل فقط الاحتيال والسرقة ونشر المــواد الإباحــية وشبكات المنحرفين جنسياً ممن يستهدفون الأحداث بل أيضاً مــنظمات الاتجــار بالمخدرات والمنظمات الإجرامية التي تُركز على استغلال ما توفره الشبكات الإلكترونية من تسهيلات وفرص أكثر مما تركز على تعطيل عمل الشبكات كما يفعل الآخرون المهتمون بهذا الأمر.

و مــن جهــة أخــرى فكــون شبكة الإنترنت يمكن استخدامها من دون معرفة المســتخدم فهذا يجعل منها قناة مثالية وجهازاً مثالياً لتنفيذ العديد من نشاطات الجــريمة المــنظمة ومفهــوم عــالم الجريمة السري يعني أنه تسود هذا العالم الضــبابية او نقص الشفافية فالسرية تشكّل عادة جزءاً رئيسياً من استراتيجية الجريمة المنظمة وشبكة الإنترنت توفر فرصا ممتازة للمحافظة على هذه السرية إذ يمكــن إخفــاء الأعمال وراء حجاب من الإغفال قد يتراوح مداه من استعمال معايــير علــم الــتحكم الإلكتروني إلى جهود متطورة لإخفاء المسار التي تتبعه المعاملات عبر الإنترنت لتصل إلى مقصدها .

تتناول الجريمة المنظمة في الأساس السعي للإفادة المادية أو تحقيق الأرباح من خــلال مواصــلة العمل بوسائل جرمية ولذا كما تستعين الشركات العادية بشبكة الإنترنــت بحثاً عن فرص جديدة لتحقيق الأرباح كذلك تفعل المنظمات الإجرامية والمــنظمات الإجرامــية ليســت اللاعبات الوحيدات في أسواق الأعمال غيــر المشروعة ولكنها تكون في أحيان كثيرة أهم اللاعبين، على الأقل بسبب تمتعها

بقـدرة أكـبر علـى المنافسة التي يوفرها لها تمكّنها من التهديد بأعمال العنف بالإضـافة إلـى ذلـك تمـيل المنظمات الإجرامية إلى مهارة كبيرة في اكتشاف واسـتغلال فـرص القيام بأعمال ومشاريع جديدة غير مشروعة في هذا السياق توفر الإنترنت والنمو المتواصل للتجارة الإلكترونية مجالات هائلة جديدة لتحقيق أرباح غير مشروعة .

خـلال السـنوات القلـيلة الماضـية ازدادت حنكة ومهارة مجموعات الجريمة المـنظمة وتجارة المخدرات فمثلاً اتبعت المنظمات الكولومبية لتجارة المخدرات الممارسات التي تقوم بها الشركات العادية لتنويع الأسواق والمنتجات واستغلت أسـواقاً جديـدة فـي أوروبـا الغربية ودول الاتحاد السوفيتي السابق وأخذت المـنظمات الإجرامـية وتجـار المخدرات تزيد من توظيف اختصاصيين ماليين لإدارة شـؤون غسل الأموال أضاف هذا العمل طبقة إضافية عازلة حول عملية غسـل الأمـوال بيـنما يـتم اسـتخدام خبراء قانونيين وماليين عارفين بخفايا المعـاملات المالـية لتوفـير ملا ذات آمنة في أماكن ومؤسسات تعمل بطريقة الأوف شور وبالمثل لا تحتاج الجريمة المنظمة إلى تطوير خبرة فنية في مجال الإنترنـت فبإمكانها أن تستخدم أشخاصاً من الخبراء في عمل الشبكة واستغلال مكامـن الضعف فيها لتنفيذ المهمات الموكلة إليهم بفعالية وكفاءة إما من خلال مـنحهم مكافآت سخية أو من خلال تهديدهم بما لا تحمد عقباه إذا لم يفعلوا أو من خلال مزيج من الأمرين معاً .

تكـون عـادة لمجموعات الجريمة المنظمة قاعدة عمل في الدول الضعيفة التي تؤمـن ملاذاً آمناً تستطيع من خلاله ممارسة عملياتها العابرة للحدود الجغرافية وفـي الواقع يوفر هذا الأمر قدراً إضافياً من الحماية من تطبيق القانون ويمكّن تلك المجموعات من ممارسة نشاطاتها بأقـل قدر من المخاطر وتتلاءم الصفات

المتأصــلة للإنترنــت كشــبكة تــتخطى حدود البلدان مع هذا النمط من النشاط الإجرامي ومع الجهد الساعي إلى تحقيق أقصى الأرباح ضمن درجة مقبولة من المخاطــر ففــي العالم الافتراضي أي في عالم الشبكات الإلكترونية لا توجد أي حــدود ويشكل ذلك مزية تجعل النشاط الإجرامي عملاً جذاباً للغاية عندما تحاول الســلطات المختصــة مراقــبة هذا العالم الافتراضي تبدو أمامها حدود البلدان ومــناطق الصــلاحيات واســعة جدا ما يجعل التحقيق في الجرم بطيئا جداً في أحسن الأحوال أو مستحيلاً في أسوأ الأحوال .

و يوجــد على شبكة الإنترنت INTERNET حوالي ٢٥٠ مائتين و خمسون موقعــا LOCATIONS خاصا بأعضاء عصابات المافيا و بعصابات المافيا نفســها و تلك العصابات تستغل تلك المواقع في إرسال خططها و تعليماتها إلى أعضــائها فــي كافــة بــلاد العالم بل أن بعض تلك المواقع يستغل في استقبال أعضــاء جــدد يريدون الانضمام إلى عالم عصابات المافيا كما أن هناك مواقع أخــري ANOTHER LOCATIONS ســمح للزوار بتصفحه لمعرفة عالم عصــابات المافيا عن قرب إلا أن معظم تلك المواقع غير مسموح بالدخول عليه إلا للأعضاء فقط .

و الجريمة المنظمة موجودة من فترة زمنية طويلة أي أنها لم تعتمد على التقدم التقنــي MODERN TECHNIQUES الحالــي في تكوينها أو إنشائها إنمــا هــي قد استغلت هذا التقدم التقني في تقوية الروابط فيما بين أعضائها و كذلــك فــي تســهيل عملية توصيل الأوامر و التعليمات إلى أعضائها بصورة مشــفرة و بالتالــي دون قلق من أي عملية تعقب قد يقوم بها أي جهاز قانوني محلى أو دولي لأعضائها أو لقياداتها .

و بعض المتخصصين في مجال الجريمة المنظمــــة يربط بينها و بين الإرهاب

على أساس أن أساس عمل كلاهما هو إفشاء الخوف و الترويع فيما بين الناس كما أن هناك توافق كبير جدا في طريقة العمل و أساليب التنفيذ مما أدى بهؤلاء الخبراء إلى الاعتقاد إلى وجود تناسق كبير و تخطيط مشترك فيما بين كل من أعضاء منظمات الجرائم المنظمة و الإرهابيين فالإرهابيين يستفيدون من خبرة هؤلاء الأشخاص في تنفيذ مخططاتهم و العكس صحيح فأعضاء منظمات الجرائم المنظمة يستفيدون من الإرهابيين الأموال الطائله منهم مقابل تنفيذ مخططاتهم ٠

التكييف القانوني للجريمة

في الكثير من الدول تم مواجهة تلك العصابات المنظمة و الذين يقومون بارتكاب الجرائم الكبرى من خلال تشريعات خاصة تم وضعها لمواجه تلك العصابات ٠
الجريمة المنظمة لم تكن ضمن الجرائم المعروفة في الماضي و عليه فلا توجد أي من القواعد القانونية في مصر و التي يمكن أن تجرمها على أساس أن مرتكب تلك الجريمة هي عصابة منظمة إلا انه يمكن تجريم أي جريمة ترتكب على أساس انها جريمة قد ارتكبت من قبل عدد من الأشخاص و يتم العقاب فيها على أساس أنها ارتكبت من عدد من الأشخاص دون أن يكون لكون مرتكبها إحدى العصابات المنظمة عاملا مشددا في العقاب ٠

خامسا – تجارة المخدرات
TRAFFICKING OF DRUGS

تعد تجارة المخدرات هي أحد أهم و اخطر أنفسهم التجارة المحرلمة على مستوى العالم و يأتي بعدها تجارة الرقيق الأبيض ثم تجارة السلاح ٠

فتجارة المخدرات هي اكثر أنفسهم التجارة المحرمة انتشارا على مستوى العالم و لـم تفلح كافة الجهود المبذولة على مستوى العالم إلا في تقليلها دون القدرة علـى مـنعها نهائـيا نظرا لوجود بعض دول العالم التي تتركز فيها تصنيع و تهريـب تلـك المخـدرات إلـى باقي دول العالم و لما تدره تلك التجارة على العاملين فيها من ربح وفير ٠

وقـد كـان تجـار المخـدرات يلاقون صعوبات كثيرة في الاتفاق على عمليات التهريـب علـى مسـتوى العـالم إلا انه و بعد التطور التكنولوجي الكبير على مستوى العالم و المتمثل في انتشار شبكة الإنترنت فقد استغل مصنعي و مهربي المخـدرات شـبكة الإنترنـت و اسـتخدموها في الاتفاق على عمليات تهريب المخدرات من بلد إلى آخر ٠

إلا أن الإنترنت قد ساهمت أيضا في الترويج لتناول المخدرات و هو نشاط آخر قـام بـه تجار المخدرات على مستوى العالم ليزيدوا من السوق الاستهلاكية و الطلب على منتجاتهم ٠

و فـي تقرير نشرته شبكة C N N الإخبارية (WWW.CNN.COM) ذكـرت فـيه قيام السلطات الاتحادية و المحلية في عدد من الولايات الأميركية بحملـة واسعة بهدف تعقب مروجي المخدرات الذين يوزعون العقار المخدر المسـمي GHB عـبر الشبكة الإلكترونية (الإنترنت - INTERNET) وألقـت القـبض على العشرات منهم في مختلف المدن الأميركيـة وذلك في محاولـة مـن السـلطات في الحد من انتشار هذا العقار المخدر لما له من آثار مدمرة على الجهاز العصبي لمن يتعاطاه .

وفـي أول حملـة من نوعها قام المحققون بما يزيد عن ١٥٠ حملة تفتيش في أكـثر مـن ٧٠ مديـنة أميركية اعتقل فيها العديد من موزعي المخدرات الذين طوروا في أساليب نشاطهم الممنوع قانونا و اصبحـوا يستخدمون تكنولوجيا

العصر الإنترنت لتوزيع بضائعهم المخدرة .

وقـال مصـدر في السلطات الاتحادية في الولايات المتحدة الأمريكية أن الحملة التـي اسـتغرقت عامـان تقريـبا تستهدف مبدئيا خمسة و عشرون من تجار المخدرات الذين يديرون تجارتهم عبر شبكة الإنترنت INTERNET الخاصة بهم والتي تمكن الزبائن من الدخـول إلى الموقـع وتحديد طلباتهـم من مخدر (GHB) والأنـواع المخـدرة الأخرى التي يتاجرون فيها و التي ترسل إليهم عبر البريد .

وشـارك قسـم مراقـبة الـبريد الأميركي ودائرة الجمارك ومكتـب التحقيقات الفيدرالـية الأمريكي (F P I) في تلك الحملة التي قادت إلى الكشف عن هـؤلاء الأشـخاص الذيـن يـتاجرون فـي المخـدرات عـبر شبكة الإنترنت INTERNET و كذلـك عن المواقع SITES التي يستخدمونها في نشاطهم المشبوه .

و(GHB) هـو عقـار مخـدر عـبارة عن خليـط يتكون من مواد كيمائية صـناعية وكان الكونغرس الأميركي قد اصدر قانوناً بتحريمها قبل عدة سنوات ويعمـل هذا العقار المسمي (GHB) و كذلك مشتقاتـه GBL , 1K4 BD كعـامل مؤثر على النظام المركزي للأعصاب مما يتسبـب في الشعـور بالدوار والغثـيان و الدوخـة وعدم القدرة على التركيز و قد قدرت الأجهـزة الأمنيـة الأمريكـية أن هـذا العقـار المخـدر و المسمي عقار (GHB) و كذلـك مشـتقاته قـد تسببت في وفـاة أكثر من اثنان و سبعون شخصاً وفقاً للأوراق الرسميـة .

وتحاول الأجهزة الأمنية والحكومية الأميركية عقد دورات تثقيفية تهدف لتحذير الجمـيع بصفة عامة و النساء بصفة خاصة من الوقوع في فخ المروجين الذين يخلطون المواد المخدرة بالمشروبات .

التكييف القانوني للجريمة

تعـد جريمة الاتجار في المخدرات إحدى اقدم الجرائم المنصوص على تجريمها فـي كافـة قوانيـن دول العالم بل والأكثر من ذلك أن تصنيعها أو زراعة أحد النـباتات التـي تسـتخرج منها أو توزيعا أو إخفائها أو أي أعمال من الأعمال المتصلة بما تم ذكره هو عمل مجرم و مشددة عقوبة القيام به ٠

و في مصر أيضا تعد جريمة الاتجار في المخدرات من الجرائم المنصوص على تجريمها بل أن جمهورية مصر العربية قد شددت في عقاب من يجلب المخدرات من الخارج محاولا إدخالها مصر بالإعدام شنقا متى ثبتت التهمة في حقه ٠

سادسا – غسيل الأموال

غسيل الأموال يعنى في ابسط صوره هو تحويل المصدر غير المشروع للأموال إلـى مصـدر مشـروع فمثلا تحويل الأموال الناتجة من عمليات غير مشروعة كتجارة المخدرات إلى أموال مصدرها مشروع كتجارة السيارات مثلا ٠

و مصـطلح غسيل الأموال هو مصطلح حديث إلى حد ما و قد بدا استخدام هذا المصـطلح فـي الولايـات المتحدة الآلي عام ١٩٣١ م حيث تمت محاكمة أحد زعمـاء المافـيا و مصـادرة أموالـه على أساس أن مصدرها هو تجارة غير مشروعة (تجارة المخدرات)

و نحن نرى انه يمكن تعريف مصطلح غسيل الأموال بأنه : –

(تحويل مصدر الأموال غير المشروع إلى مصدر مشروع)

و قـد أعطـت شبكة الإنترنت عدة مميزات لمن يقومون بعمليات غسيل الأموال منها السرعة الشديدة و تخطى الحواجز الحدوديـة بين الدول و تفادى القوانين

التي قد تضعها بعض الدول و تعيق نشاطهم وكذلك تشفير عملياتهم مما يعطيها قدر اكبر من السرية ٠

و أيضـا كـان انتشـار الـتجارة الإلكترونـية الإلكتروني SIGNATURE ELECTRONIC عـبر شـبكة الإنترنـت INTERNET خير المعين لهـؤلاء القائميـن على عمليات غسيل الأموال فالتجارة الإلكترونية و انتشارها عـبر أنحاء العالم اجمع قد ساعد كثيرا في عمليات غسيل الأموال نظرا لسرعة الاتفاق على الصفقات و إتمامها من خلاله دون أن تكون في معظم الأحيان تحت رقابـة قانونـية صارمة بل انه في حالة وجود رقابة قانونية يكون من الممكن تفـادى تلـك الرقابة و إتمام تلك الصفقات عبر الاتفاق على خطوات و ترتيبات تنفـيذها عبر الإنترنت و بطريقة تشفير معقدة لا يمكن حلها و بالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفقات ٠

كذلـك سـاهمت بعـض الجـرائم التي ترتكب عبر الإنترنت INTERNET CRIMES مـثل تزوير البيانات FORGERY OF DATA و المواقع الافتراضية (الغير حقيقية) تعد أيضا من العوامل المساعدة التي وفرتها شبكة الإنترنت للقائمين على عمليات غسيل الأموال ٠

التكييف القانوني للجريمة

تعتبر جريمة غسيل الأموال هي من الجرائم الحديثة و قد قامت العديد من الدول أما بتعديل نصوصها لتستوعب تجرين تلك الجريمة الجديدة أو بتشريع نصوص جديدة تجرمها ٠

وفـي مصـر تم تشريع قانون جديد يجرم جريمة غسيل الأموال و يعاقب عليها بأشد العقوبة نظرا لما تسببه من سمعة سيئة للبلاد و تقويض الاقتصاد الوطني المصري ٠

سابعا : المواقع المعادية

مصطلح المواقع المعادية أيضا هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي الذي نعيشه حاليا و مصممي تلك المواقع المعادية قد استغلوا تلك التكنولوجيا لخدمة أغراضهم الشخصية في عرض أفكارهم الشخصية المغرضة التي لم يمتلكوا الشجاعة الكافية في سلك الطرق الشرعية المباحة في عرض تلك الأفكار و الآراء .

و تلك المواقع المعادية قد يكون الغرض منها : -

- ١ - الإساءة إلى دين معين من الأديان و نشر الأفكار السيئة عنه و حث الناس على الابتعاد عنه و تلك المواقع غالبا ما يكون القائمين عليها من معتنقي الديانات الأخرى المتشددين في دينهم الذين لا يعتنقون فكرة التسامح و التعايش بين الأديان أو أن يكون هدفهم بث الشقاق فيما بين أفراد الشعب الواحد و المعتنقين لأكثر من دين فيحاولون إثارة الفتنة فيما بينهم عن طريق نشر الأخبار الكاذبة و المضللة في محاولة منهم لتحقيق هدفهم الخبيث .
- ٢ - الإساءة إلى بلد معين و إلى مواقف قادته السياسيين من قضاياه الوطنية وهم غالبا ما يكونون من معارضي النظام السياسي القائم في بلد ما فيحاولون نشر الأخبار الفاسدة التي تنشر الفرقة فيما بين أفراد الشعب و نظامه السياسي القائم .
- ٣ - الإساءة إلى شخص معين بما يمثله من مواقف سواء دينية أو سياسية أو وطنية

أو ما إلى ذلك من الأهداف التي لا يجد القائمين عليها من يستمع إلى آرائهم

المغلوطـــة أو التـــي تتـــنافى من الدين و المبادئ و عليه يجد هؤلاء في شبكة الإنترنـــت ضـــالتهم المنشودة في الوصول إلى اكبر عدد من الأشخاص لعرض آرائهـــم عليهم في محاولة منهم لكسب تأييدهم دون تعريف أنفسهم في محاولة منهم للتخفي خوفا من رد فعل الناس التي غالبا ما ترفض مثل تلك الآراء التي بـــدلا مـــن يجاهـــر أصحابها بها و اتخاذهم الطريق القانوني الصحيح في نشر أفكـــارهم و آرائهـــم ليكون من حق أفراد الطرف الثاني عرض وجهة نظرهم و ردهـــم على تلك الاتهامات نجد انهم يتخوفون و يتخفون دون أن يمتلكوا أنواع شجاعة في الإعلان عن أنفسهم و في عرضهم لآرائهم .

التكييف القانوني للجريمة

نقض المواقف السياسية للدولة لمحاولة الوصول إلى السياسة الصحيحة و دون أدنـــي تعـــرض للشخصـــيات و الأعراض هو من الأمور الغير معاقب عليها أما الـــتعرض للشخصـــيات العامة و انتهاك حرماتهم و التشكيك في أخلاقياتهم فهو من الأمور المجرمة في كافة القوانين .

أمـــا الـــتعرض للأديـــان فهو من الأمور المجرمة و الغير مقبولة على الإطلاق خاصـــة فـــي البلاد الإسلامية التي يحث الدين الإسلامي وهو الدين الغالب فيها على احترام الأديان الأخرى و عدم التعرض لمعتنقي أي دين اخر .

و فـــي مصر لا تزال القوانين القديمة هي السائدة ولم يتم تعديل أي من قواعد قانون العقوبات ليشمل أي من تلك الجريمتين بطريقة صريحة .

و نحن لا نريد فقط تعديل قانون العقوبات المصري ليشمل تلك الجريمتين بل و لـــيجرم بشـــكل صريح كافة الجرائم الإلكترونية الأخرى دون أن يوضعوا تحت قواعـــد قديمـــة لا تتناسب العقوبات المقررة فيها تلك الخسائر و الأضرار التي

تتسـبب فيها تلك الجرائم فنحن نريد عقوبات مشددة جدا تتناسب مع ما تسببه تلك الجرائم الإلكترونية الحديثة من أضرار •

ثامنا : جرائم القرصنة
PIRACIES CRIMES

لقـد وفرت شبكة الإنترنت في ظل ما توفره من تقنيات حديثة MODERN TECHNIQUES - لكونهـا تـربط العالم اجمع و تلغى الحدود الجغرافية ممـا أتـاح فرصـة ارتكـاب الجرائم عابرة الحدود CRIMES TRANS BORDER فـي أوقـات قياسية و بأقل قدر من المخاطرة RISKING - مجـالا خصـبا لنمو نوع جديد من أنواع الجرائم لم يكن معروفا في من قبل ألا وهـو الاسـتخدام غـير المشروع - النسخ غير المشروع - لنظم تشغيل و لبرامج الحاسب الآلي COMPUTER •

فمـن المعـروف أن النسـخ غير القانوني لنظم تشغيل و برامج الحاسب الآلي تـؤدى إلـى خسـائر رهيبة لمنتجي تلك البرامج و نظم التشغيل كما أن جرائم القرصنة على البرامج الأصلية ORIGINAL PROGRAMS تؤدى إلى إبطاء عمليات التطور و البحث العلمي لتلك الشركات المنتجة لتلك البرامج نظرا لخسـائرها الماديـة الباهظة نتيجة جرائم القرصنة تلك التي تقع على برامجها التـي أنتجـتها و أنفقت على تطويرها و إنتاجها الكثير معتمدة على ما ستجنيه من أرباح يعمل على تعويض كل ما أنفقته •

و جـرائم القرصـنة التي تتم عبر شبكة الإنترنت INTERNET لا تقع فقط علـى بـرامج تشـغيل الحاسب الآلي COMPUTER و إنما تقع على أي منتجات فكرية أخرى إذ يتم نسخها •

و تشـــير التقديرات إلى أن هناك حوالي ٣٠٠ مليار صفحة على الأقل يتم إعادة إنـــتاجها مـــن خـــلال آلة نسخ واحدة كل سنة على مستوى العالم ويشمل هذا النسخ الصحف والمجلات و النوت الموسيقية (J.W. Rodlop 99) .

طبعا هذا الرقم يشمل القرصنة (PIRACIES CRIMES) التي تتم مقابل الـــربح المـــادي و أيضـــا القرصنة التي تتم و لكن دون أن يكون هدفها تحقيق الـــربح المـــادي فالنســـخ للاســـتخدام الداخلي كالمعاهد والجامعات والمدارس والمؤسســـات التعليمـــية والمستشـــفيات بشكل عام وحتى المنازل يمكن لهم أن ينسخوا لأغراض داخلية وشخصية .

و لـــم يعد النسخ هذه الأيام مقصورا على آلات التصوير التقليدية فاليوم أصبح النسخ الرقمي الذي يمكن أن يمسح من خلالها ضوئيا ويخـــزن رقميا باستخدام النسخ عبر الليزر وكذلك الأمر بالنسبة لأسلوب النسخ الألكتروستاتيكي الجاف (COPYING DRY ELECTROSTATIC) والذي يمكن أن يستوعب (٦٠٠*٤٠٠ فـــي كـــل بوصة) حيث يمكن بعد ذلك بثها في الشبكات وتوسيعها ومسحها ضوئيا وإعادة طباعتها من خلال كمبيوتر وطابعة عادية وقد تكون في بعض الحالات الأعمال المنسوخة أفضل نوعية من الأعمال الأصلية .

(J.W.RUDOLPH ١٩٩٩) .

لقـــد بـــات النســـــخ (COPY) بـــدون إذن أو ترخيص إلى جانب السلبيات والمخـــــاوف التـــي تخلفها التجارة الإلكترونية يزعج ويقلق مالكي البرامج و منتجـــيها و الناشرين والمؤلفين وأصبحت التكنولوجيا المتقدمة ومصدر إزعاج لمالكـــي الحقـــوق الفكـــرية والمعـــنويـــة مما دعاهم إلى التفكير بتشكيل إدارة جماعـــية لهذه الحقوق و إحاطة هذه الحماية بأطر قانونية عن طريق المعاهدات الدولـــية لتتمـــتع بالحمايـــة القانونيـــة من أجل استغلال هذه الحقوق في عقود الترخيص على غرار عقود الترخيـــص الخاصـــة باستعمال علامة تجاريـــة أو

استغلال براءة أختـــراع .

و يـــتذمر مـــالكو الحقـــوق الفكـــرية والمعنوية ليس فقط من القوانين المحلية والقصـــــور في تطبيقها بل حتى من قصور آليات حسم المعاهدات الدولية حيث أن هـــذه المعـــاهدات وتلـــك القوانين كانت قد وضعت عندما كانت الطباعة تتم بالنســـخ باليد أو بالآلة الطابعة العادية وقبل أن يكون هناك آلات تصوير ونسخ باللـــيزر والتـــي أصـــبحت تمكن المستعملين والدارسين من حيازة نسخ الكتب والأبحـــاث عـــن طـــريق تصويرها ونسخها في المكتبات العامة أو الجامعات أو المعاهد أو المدارس أو الشركات لإعادة إنتاج نسخ مجانية لغايات إيضاح التعليم وتسهيلـــــه .

هـــذا مـــن جهـــة ومن جهة أخرى فإن العولمة التجارية وزيادة استعمال التجار والمســـتثمرين الشبكات الدولية والبريد الإلكتروني (E - MAIL) وتبادل رســـــائل البـــــيانات إلكترونـــــيا ELECTRONIC DATA INTERCHANGE (EDI) و تحـــول الكثير من الحكومات إلى ما يسمى بالحكومـــة الإلكترونـــية ELCTRONEC GOVERNMENTS أدى إلـــى زيـــادة اهـــتمام المجـــتمع الدولـــي بالضـــوابط القانونيـــة للتجارة الإلكترونية ELECTRONIC COMMERCE وهـــذا ما تنبهت له الجمعية العامة فـــي الأمـــم المتحدة فوضعت عام ١٩٩٦ قانونا نموذجيا للتجارة الإلكترونية (لقـــانون الأونســـترال UNCTTRAL LAW) لـــتقوم الـــدول الأعضاء بالاسترشاد به .

و قـــد أدت قرصـــنة الـــبرامج إلـــى خسائر مادية باهظة جدا و صلت في عام ١٩٨٨ م إلـــى حوالـــي إحـــدى عشر مليار دولار أمريكي في مجال البرمجيات وحدها و لذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد و إنشاء منظمـــة خاصـــة لمراقبـــة و تحليل ســـوق البرمجيات و من ذلك منظمة اتحاد

برمجيات الأعمال (BUSINES SOFTWARE ALLIANCE) أو ما يعــرف اختصـــارا بــ (B S A) و التي أجرت دراسة تبين منها أن القرصنة علـــى الإنترنـــت ستطغى على أنواع القرصنة الأخرى و دق هذا التقرير ناقوس الخطــر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادى القرصنة على الإنترنـــت و مـــنها تهديـــد بعـــض الشركات بفحص القرص الصلب لمتصفحي مواقعهــم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج القرصنة إلا أن تلـــك الشركات قد تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت •

التكييف القانوني للجريمة

تدخـــل جرائم القرصنة ضمن نطاق جرائم السرقة و عليه فكل القواعد القانونية التي تنطبق على السرقة تنطبق على جرائم القرصنة •

تاسعا : جرائم التجسس الإلكتروني
CRIMES OF THE ELECTRONIC ESPIONAGE

عمليات التجسس هي عمليات قديمة قدم البشرية و قدم النزاعات البشرية فمنذ تقدم العصور كان الإنسان يتجسس على أعداءه لمعرفة أخبارهم و الخطط التي يعدونهـــا لمهاجمـــته و لهـــذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة •

و قـــد تطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية و تكنولوجية •

فمثلا اختـــرع الإنسان جهاز الرادار ليتجســـس على أعدائـــه و معرفـــة كافـــة

تحـــركاتهم ثـــم حـــدث تطور كبير ألا وهو اختراع الأقمار الصناعية التي تقوم بتصوير الإنسان و الآلات الحربية و المدنية و المباني و كل ما هو فوق الأرض يـــتم تصويره كل فترة زمنية معينه لمعرفة التحركات التي تتم و الآن و في ظل الـــتطور التقنـــي الهـــائل الـــذي نعيشـــه فقد اصبح هناك ما يعرف بالتجسس الإلكتروني ٠

و التجســس الإلكترونـــي ELECTRONIC ESPIONAGE لا تكمـــن خطورته إذا ما كان القائم به هم بعض الهواة العابثين HACKERS و كان الغرض من اختراقهم لأجهزة الحاسبات الآلية COMPUTERS و الشبكات NETWORK هو العبث بالمحتويات أو إلغاء DELETE بعضها أو كلها إلا أن الأهمية تكمن فيما إذا كان القائم بتلــك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على الدول الأخـــرى ٠

و قد وجدت بعض حـــالات التجسس الدولي و منها ما اكتشف أخيرا عن مفتاح وكالـــة الأمـــن القومي الأمريكية (N S A) و التي قامت بزراعتـــه في نظام التشـــغيل الشهير (ويندوز – WINDOWS) و ربما يكون هـــذا هـــو أحد الأسباب الرئيسيـــة التي دعت الحكومة الألمانية بإعلانها في الفترة الأخيرة عن استبدالها لنظام التشغيل (ويندوز – WINDOWS) بأنظمة تشغيل أخرى ٠

كمـــا كشـــف أخـــيرا الـــنقاب عـــن شـــبكة دولية ضخمة للتجسس الإلكتروني ELECTRONIC ESPIONAGE تعمـــل تحـــت أشـــراف و كالة الأمن القومي الأمريكية (N S A) بالتعاون مع أجهزة الاستخبارات و التجسس في كـــل مـــن كندا و بريطانيا و نيوزيلندا و يطلق عليها اسم (ECHELON) لرصـــد المكالمات الهاتفية و الرسائل بكافة أنواعها سواء ما كان منها برقيا أو تلكس أو فاكس أو إلكترونيا ٠

و خصـــص هـــذا النظام للتعامل مـــع الأهداف الغير عسكرية و بطريقة تجعله

يعـترض كمـيات هائلـة جـدا من الاتصالات و الرسائل الإلكترونية عشوائيا باسـتخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة و التي تم إنشاء العديـد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية و منها محطة رصد الأقمار الصناعية الواقعة في منطقة (واى هوباى) بجـنوب نيوزيلندا و محطة (جيرالدتون) الموجودة بأستراليا و كذلك المحطة الموجـودة فـي مـنطقة (موروينستو) بمقاطعة (كورنوول) في بريطانيا و المحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة (شوجر جروف) وتبعد حوالـي مائتـي و خمسون كيلو مترا جنوب واشنطن و كذلك المحطة الموجودة بولاية واشنطن على بعد مائتي كيلو مترا جنوب غرب مدينة سياتل ٠

ولا يقتصر الرصد على المحطات المرتبطة بالأقمار الصناعية و الشبكات الدولية الخاصـة بالاتصـالات الدولـية بل يشمل أيضا رصد الاتصالات الأرضية و كذا الشبكات الإلكترونية أي انه يرصد جميع الاتصالات التي تتم بأي وسيلة و يعتبر الأفراد و المنظمات و الحكومات اللذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمـة كوديـة لحمايـة شـبكاتهم و أجهـزتهم أهدافا سهله لشبكة التجسس الإلكترونـي ELECTRONIC ESPIONAGE هـذه و أن كان هذا لا يعـنى بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام مـن الغـزوات الاستخباراتية لهذه الشبكة و مثيلاتها ولا يقتصر التجسس على المعلومـات العسـكرية أو السياسـية فقط بل تعداه إلى المعلومات التجارية و الاقتصادية بل و حتى الثقافية ٠

فمـع توسـع الـتجارة الإلكترونية ELECTRONIC COMMERCE عـبر شبكة الإنترنت INTERNET تحولت الكثير من مصادر المعلومات إلى أهـداف للتجسـس الـتجاري ففي تقرير صدر عن وزارة التجارة و الصناعة البريطانيـة أشار إلى زيادة نسبة التجسس على الشركات من (٣٦ %) عام

١٩٩٤ م إلـــى (٤٥ %) عام ١٩٩٩ م كما اظهر استفتاء أجرى عام ١٩٩٦ م لمســـئولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول و بشـــكل غـــير مشـــروع علـــى معلومات سرية لأنشطة تجارية و صناعية في الولايات المتحدة الأمريكية ٠

و مـــن الأســـاليب الحديـــثة فـــي التجسس الإلكتروني ELECTRONIC ESPIONAGE أســـلوب إخفـــاء المعلومـــات داخل المعلومات وهو أسلوب شـــائع و أن كـــان ليس بالأمر السهل و يتلخص هذا الأسلوب في لجوء المجرم إلـــى إخفـــاء المعلومـــة الحساسة المستهدفة بداخل معلومة أخرى عادية داخل الحاسب الآلي و من ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها و الغير عادية في داخلها و بذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريـــبها حتى ولو تم ضبط الشخص متلبسا فمن الصعب جدا الوصول إلى تلك المعلومات المغلفة في معلومات أخرى غير مشكوك فيها على الإطلاق ٠

و مـــن احـــدث و اشـــهر أمـــثله التجسس الإلكتروني ELECTRONIC ESPIONAGE انه بعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية في سبتمبر صدرت تعليمات جديدة لأقمار التجسس الأمريكية الصناعية بالتركيز على أفغانستان و البحث عن أسامة بن لادن و الجماعات التابعة و الموالية له و قـــررت الســـلطات الأمريكـــية الاستعانة في عمليات التجسس على أفغانستان بقمرين صناعيين مصممان خصيصا لالتقاط الاتصالات التي تجرى عبـــر أجهزة اللاســـلكي و الهواتـــف المحمولة بالإضافة إلى قمرين آخرين يلتقطان صـــورا فائقـــة الدقـــة و فـــي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاســـتعانة بقمريـــن تابعيـــن لها لرصد الاتصالات و من ثم تحول بعد ذلك إلى الولايـــات المتحدة الأمريكية حيث تدخل في أجهزة كومبيوتر COMPUTER متطـــورة لتحليلها ٠

التكييف القانوني للجريمة

جــرائم التجسس جرائم قديمة و معاقب عليها بأشد العقوبات في كافة القوانين القديمة و الحديثة ٠

و التجســـس الإلكترونـــي هــو أحد أشكال التجسس الحديث كالتجسس بواسطة الأقمـــار الصـــناعية و التجسس بواسطة طائرات الاستطلاع المتقدمة إلا انه في معظم الأحيان لا تتمكن الدولة – رغم علمها بأسم الدولة التي تتجسس عليها – مــن ضــبط الشخص الذي يقوم بالتجسس إلا في أحوال معينه وهى إذا ما كان التجســـس يــتم بالشكل القديم و الذي يتم بأرسال شخص من الدولة إلى الدولة الأخـــرى للحصـــول على المعلومات من مصادره في تلك الدولة فيتم التمكن من ضبطه ٠

عاشرا : الإرهاب الإلكتروني
THE ELECTRONIC TERRORISING

فـــي الماضـــي كان الإرهاب TERRORISING يعنى قيام بعض الإرهابيين بتفجير قنبلة في مكان ما أو اغتيال شخصية ما أو تفجير طائرة في الجو و ما إلى ذلك من عمليات روتينية اعتاد رجال الأمن في جميع الدول على مواجهتها و كانـــت تلـــك العملـــيات تتم بغرض نشر الإرهاب في الدولة التي ينتمي إليها الإرهابييـــن أو حـــتى فـــي دولة لا ينتمون إليها لتحقيق أغراضهم و التي كان معظمها يتمثل في معارضة النظام الحاكم و ما يمثله من رموز أو تحجيم الحركة الســـياحية أو اغتـــيال رمـــوز فكرية تتناقض أفكارها مع فكر الإرهابيين الذين يقومون بتنفيذ تلك العمليات و ما إلى ذلك من أهداف ٠

أما الآن و مـــع التقدم التقني MODERN TECHNIQUES و مع تقدم

وســـــائل الاتصـــــالات MODERN COMMUNICATION TECHNIQUES الــذي نعيشه و نكاد نلمسه فقد تغيرت و تطورت تلك الأســاليب SYSTEMS التي يحاول الإرهابيين بها الوصول إلى أهدافهم فقد اصـبح الإرهــاب الإلكترونـــي هــو الســائد حاليا و اصبــح اقتحام المواقع STORMING SITES و تدمــيرها DISTROYING IT و تغيـــير محــتوياتها و الدخول على الشبكات و العبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على شبكات الطاقــة أو شبكات الاتصالات بهدف تعطيلها عن العمــل أطــول فــترة ممكــنــة أو تدميرها نهائيا اصبح هو أسلوب الإرهاب SYSTEMS OF TERRORISING حالــيا فـــي محاولــة الوصول إلى أغراضهم ٠

و نحــن نــرى الآن أن الإرهــاب TERRORISING الــذي تمارسه دولة إسرائيل ضد الشعب الفلسطيني PALESTINIAN PEOPLE لا يتمثل فقط فـــي اغتـــيال رموزه بل و أفراد شعبه و تشريد شعبه و استيلاءه على أرضه و ممــتلكاته و ما إلى ذلك و إنما الإرهاب الذي تمارسه دولة إسرائيل امتد ليشمل الإرهــاب الإلكترونـــي فــالمواقع الفلسطينية PALESTINIAN SITES علـــى شبكة الإنترنت ON THE INTERNET تتعرض و بصفة مستمرة من الإسرائيليين إلى الاقتحام و العبث بمحتوياتها و إزالة ما عليها من معلومات و عــرض صــورة العلــم الإسرائيلي على الصفحة الرئيسية MAIN PAGE بــالمواقع المقــتحمة THE STORMED SITES و فـــي المقابل يحاول الفلســطينيين معالجـــة تلـــك الآثــار و تصحيح و إزالة العبث الواقع على مواقعهــم و أيضـــا يحــاولون اقــتحام بعض المواقع الإسرائيلية و وضع العلم الفلســطيني PALESTINIAN FLAG على الصفحة الرئيسية MAIN PAGE بها في المقابــل ٠

و هـــذا الإرهــاب THISE TERRORISING لا تقتصــر ممارســته على الإســرائيليين الموجوديـــن بإســرائيل فقــط و كذلك الفلسطينيين الموجودين بداخــل فلســطين فقـــط و إنمــا امــتد الوضع ليشمل كل من الإسرائيليين و الفلسطينيين الموجودين بالخارج فكل منهم يقوم بمساعدة بلده فاليهود يحاولون مســاعدة إســرائيل علــى استمرار احتلالها لفلسطين و الفلسطينيون يحاولون مساعدة ذويهم بالدخل - داخل فلسطين - في مقاومة الاحتلال INVASION الإســرائيلي وقــد وفرت لهم شبكة الإنترنت - التي ألغت الحدود الجغرافية بين الــدول و - تلــك المساعدة التي اصبح في إمكانهم القيام بها من خارج حدود دولــتهم - وهو ما ساعد كثيرا الفلسطينيين الموجودين بداخل فلسطين المحتلة فــبعد أن كــانوا بمفــردهم وجهــا لوجه مع المحتل اصبحوا يجدون المعاونة الخارجية المؤثرة و المفيدة لهم .

التكييف القانوني للجريمة

كافــة بــلاد العالم اصبح لديها قوانين خاصة بمكافحة الإرهاب و لكن كل دولة علــى حدة نظمته بما يتناسب مع ظروفها الاجتماعية و مع درجة شدة الإرهاب الذي تعانيه .

و كــان العالم العربي على قدم المساواة مع العالم الخارجي في تقنين تشريعات جديــدة أو تعديــل مــا لديه من تشريعات ليكون لديه القواعد القانونية الكافية لــيحارب الإرهــاب الذي يعانيه العالم اجمع إلا أن العالم العربي لما هو معروف عــنه الســماحة و الخلــق القويــم لا يعانى من الإرهاب كما يعانى منه العالم الخارجي .

الفصل الثالث

مكافحة الجرائم الإلكترونية

STRIVING THE INTERNET CRIMES

أن مكافحة الجرائم الإلكترونية لن يكون له أي تأثير يذكر إلا إذا كان هناك تعاونا دوليا على اكبر قدر من التنسيق و التعاون و عليه يمكننا القول أن أي مجهود أو إجراءات قد نقوم بها أي من الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم فتلك الجرائم لها طابع خاص تتسم به هو أنها جرائم عابرة للحدود فهي لا تتم من داخل دولة و يكون تأثيرها منحصر في تلك الدولة و إنما تلك الجرائم ترتكب في عبر عدد من الدول لتتم في دول أخرى و تكون آثارها ممتدة لتصل إلى عدد غير محدود من الدول و عليه فأن الأساس الذي يرتكز عليه مجال مكافحة الجرائم الإلكترونية هو التعاون الدولي و تنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الارتكاز عليها و تقويتها للحد من تلك الجرائم ذات النتائج البشعة على الاقتصاديات الدول و الكيانات الاقتصادية ٠

و عليه فسوف يكون تناولنا لمكافحة الجرائم الإلكترونية من خلال التركيز على التعاون الدولي و العناصر التي يرتكز عليها هذا التعاون و التي تنحصر في الآتي : -

- ١ - المعاهدات و المؤتمرات الدولية ٠
- ٢ - إصدار قوانين جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق ٠
- ٣ - التعاون الدولي ٠
- ٤ - اتحاد الشركات و الكيانات الاقتصادية الكبرى في مجال حماية أمنها الإلكتروني ٠

- ٥ – المعاهدات و القوانين الخاصة بحق الملكية الفكرية ٠

١ – المعاهدات و المؤتمرات الدولية

تعـد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحـة الجرائم الإلكترونية و قد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية و من تلك المعاهدات

أ – معاهدة بودابست لمكافحة جرائم الإنترنت

THE BUDAPEST CONVENTION ON CYBER CRIMES

شـهدت العاصـمة المجـرية بودابسـت فـي أواخر عام ٢٠٠١ م ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت INTERNET CRIMES و تـبلور التعاون و التضامن الدولي في محاربتها و محاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير اصبح يهدد الأشخاص و الممتلكات ٠

و يعـد التوقـيع علـى تلـك المعاهدة دولية – التي تهدف إلى توحيد الجهود الدولـية فـي مجال مكافحة جرائم الإنترنت INTERNET CRIMES و التـي انتقلـت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم من الحالات و دون أي غرض إجرامي إلى إلـى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص و تتمثل فـي الاحتـيال والاخـتلاس وجـرائم تهديد الحياة وهي قضايا تعرض حياة و ممتلكات الكثيرين من رواد شبكـة الإنترنت للخطر – هو الخطوة الأولى في

مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت و استخدامها الاستخدام الأسوأ ٠

و يعـد التوقـيع على تلك الاتفاقية - من المسئولين في الدول الأوربية إضافة إلـى أمريكا و اليابان و كندا و جنوب أفريقيا - هو نتاج مباحثات و مفاوضات استغرقت اكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لـتلك الاتفاقـية حـتى يـتم التوقيع عليها من جميع الأطراف دون أن تجد أي اعـتراض من أي منهم بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائـرة الـدول التي توافق على الانضمام إلى تلك الاتفاقية و يتم توسيع الاتحاد الدولـي و التضامن الدولي في مجال مكافحة جرائم الإنترنت INTERNET CRIMES ٠

و قد أجريت العديد من الدراسات على مجال التضامن الدولي في مكافحة جرائم الإنترنـت أوضحت أن العديد من الدول لا تستطيع بمفردها مواجهة تلك الجرائم التي ترتكب عبر الإنترنت مهما سنت من قوانين و مهما غلظت من عقوبات تلك الجـرائم نظـرا لكون تلك الجرائم هي من الجرائم عابرة الحدود CRIMES TRANS BOEDER التي لا يقف أمامها أي عائق جغرافي و بالتالي فتلك الـدول تفضـل الانضمام إلى المعاهدات الدولية التي تبرم في هذا المجال نظرا لكـبر حجم الأضرار التي تصيبها سواء المادية أو لكثرة الجرائم الأخلاقية التي يـتم ارتكابهـا عن طريق الإنترنت ولان العديد من الدول حتى المتقدمة منها لا تسـتطيع مواجهة تلك الأخطار بمفردها دون وجود تعاون و تضامن دولي ليتم نجـاح أي مجهـودات تبذل في مجال مكافحة الجرائم التي ترتكب عبر الإنترنت INTERNET CRIMES ٠

وقـد ذكرت إحدى الدراسات حادثة كمثال عما يمكن أن تحدثه جريمة تتم عبر الإنترنت عندما سيطر أحدهم على نظام الكومبيوتر الخاص بمطار أمريكي و قام بإطفـاء مصـابيح الإضاءة الموجودة على ممرات الهبوط و وهو أمر يمكن أن يؤدى إلى سقوط الطائرات و وفاة الكثير من الأشخاص و بعد أن تم التكهن بأن وراء الحـادث عمل إرهابي تم اكتشاف أن وراءه مراهق من كاليفورنيا و عليه فالـتعاون الدولـي أمـر هـام جدا في مجال مكافحة تلك الجرائم ففي مثل تلك الحـالات يتسلل الجاني عبر العديد من الدول قبل أن يصل إلى نظام الكومبيوتر هذا .

وعلـيه فـأن التعاون و التضامن الدولي أمر هام جدا في مجال مكافحة جرائم الإنترنت و بدون هذا التعاون الدولي لن يكون هناك أي اثر لأي مجهود تقوم به أي مـن الـدول بمفردها نظرا لأنه سيكون عديم الفائدة و بلا اثر تقريبا و لن يؤدى إلى الحد من ارتكاب تلك الجرائم التي تكون في الأغلب الأعم من الحالات جرائم عابرة للحدود CRIMES TRANS BOEDER .

هـذا من جهة و من جهة أخرى فحتى الجرائم التقليدية التي تتم عبر الإنترنت مـثل النصب و الاحتيال و الاختلاس و انتهاك حقوق الملكية الفكرية فهي أيضا مـن الجرائم التي لا يمكن مواجهتها بصفة فردية كل دولة على حدة بل أن تلك الجـرائم أيضـا تحـتاج إلـى الـتعاون الدولي ليكون في الإمكان مكافحتها و مواجهـتها و محاولـة الحد من ارتكابها و ملاحقة مرتكبيها و ضبطهم لينالوا العقاب PUNISHMENT على ما اقترفت أيديهم فوضع قوانين تحمى الملكية الفكرية في كل دولة على حدة لا يكفى بأي حال من الأحوال للمحافظة على تلك الحقوق و إنما التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليتم احترام مثل تلـك الحقوق التي تجد دائما من ينتهكها أو على الأقل من يحاول

انتهاكها •

و قــد كــان الخــلاف الوحــيد فيما بين الدول الموقعة على الاتفاقية هو مجال محاربــة العنصــرية فــالدول الأوروبــية تعتــبر أن التحريض على الكراهية العنصــرية هــي جريمة INCITATION TO THE RACIALIST HATING IS A CRIME و من المعروف أن هذه الجريمة يعاقب عليها القــانون الدولــي THIS CRIME IS PUNISHING BY THE INTERNATIONAL LAW و بالتالــي فلابــد من النص في الاتفاقية على لزوم العمل على إزالة تلك المواقع التي تعمل على التحريض على الكراهية العنصــرية INCITATION TO THE RACIALIST HATING و مسائلة القائمين عليها على أساس انهم يرتكبون جريمة يعاقب عليها القانون الأوروبــي بينما الولايات المتحدة الأمريكية تعتبر أن حرية التعبير المنصوص علــيها فــي الدســتور الأمريكــي تتعارض مع ما تراه الدول الأوروبية من أن الــتحريض على الكراهية العنصرية جريمة يعاقب عليها القانون و بالتالي فهي تــرى انــه لا مجــال للــنص فــي الاتفاقية على العمل على إزالة تلك المواقع SITES على أساس أن الدستور الأمريكي لا يري في تلك المواقع أي جريمة بــل أنهــا تقوم بالتعبير عن رأيها و هو ما كفله الدستور الأمريكي إلا انه تم الاتفــاق فيما بين الجميع على عدم تضمين الاتفاقية ذلك الموضوع على أساس تقليل حدة الخلاف فيما بين الدول الأعضاء الموقعة على الاتفاقية و ذلك إلى أن يــتم دراســة الموضوع من كافة الاتجاهات و محاولة الوصول إلى نقطة وسط يتلاقى عندها كافة الأطراف •

ومــن ضــمن الجوانب العديدة التي تناولتها تلك الاتفاقية الإرهاب الإلكتروني و عمليات تزوير بطاقات الائتمان و دعــارة الأطفال و تلك الجرائم تعتبر من اكثر

الجـــرائم انتشارا على المستوى العالمة بصفة عامة و في أوربا و أمريكا بصفة خاصة و لم تفلح أي جهود فردية تم بذلها من جانب أي من الدول الموقعة على الاتفاقية و عليه فقد كان من المحتم التنسيق بين تلك الجهود على اقل تقدير أن لـــم يكن التوحيد بينها لتؤتى ثمارها في الحد من ارتكاب تلك الجرائم التي تؤثر على التقدم الاقتصادي الذي المتواصل في اقتصاديات تلك الدول المتقدمة .

وقـــد صـــاغ نصها عدد من الخبراء القانونيين في مجلس أوربا بمساعدة دول أخرى وبالأخص الولايات المتحدة .

وتحـــدد الاتفاقـــية أفضل الطرق الواجب إتباعها في التحقيق في جرائم الإنترنت INTERNET CRIMES التي تعهدت الدول الموقعة بالتعاون الوثيق من أجـــل محاربتها كما تحاول إقامة توازن بين الاقتراحات التي تقدمت بها أجهزة الشـــرطة والقلـــق الـــذي عـــبرت عـــنه المنظمات المدافعة عن حقوق الإنسان HUMAN RIGHTS والصناعات المعنية ومزودي خدمات الإنترنت .

وتخشـــى مـــنظمات حقـــوق الإنسان من أن تحد الاتفاقية من حرية الأفراد في أعقاب الهجمات على الولايات المتحدة

كمـــا أن القلـــق يتزايد من أن تؤدي زيادة الرقابة إلى انتهاك حقوق مستخدمي الإنترنت .

وهو ما يتعارض مع الإعلان العالمي لحقوق الإنسان HUMAN RIGHTS الصادر من الأمم المتحدة و الذي ينص في المادة الثانيـــة عشر منه على انه لا يـــتعرض أحـــد لـــتدخل تعســـفي فـــي حياته الخاصة أو أسرته أو مسكنه أو مراسلاتـــه .

كما أن المادة التاسعة عشر من هذا الإعـــلان تنص على انه لكل شخص الحق

في حرية الرأي و التعبير و يشمل هذا الحق حرية اعتناق الآراء دون أي تدخل و استقاء الأنباء و الأفكار و تلقيها و إذاعتها بأي وسيلة كانت دون تقيد بالحدود الجغرافية ٠

إلا أن تلك الحقوق التي نص عليها الإعلان العالمة لحقوق الإنسان الصادر من هيئة الأمم المتحدة لم يترك تلك الحقوق الإنسانية لتمارس دون أي قيود إذ انه قد نص في المادة التاسعة و العشرين على انه (يخضع الفرد في ممارسة حقوقه و حرياته إلى تلك القيود التي يقررها القانون فقط لضمان الاعتراف بحقوق الغير و حرياته و احترامها و لتحقيق المقتضيات العادلة للنظام العام و المصلحة العامة و الأخلاق في مجتمع ديمقراطي ٠

و عليه فنحن نرى أن تلك المعاهدة التي لا غرض لها إلا احترام حقوق الإنسان HUMAN RIGHTS و الحد من تعرضه للكم الهائل من الجرائم التي ترتكب عبر شبكة الإنترنت لا تتعارض بأي حال من الأحوال مع الإعلان العالمي لحقوق الإنسان الذي يعد الأساس في تقرير حريات الأشخاص ٠

ب - المعاهدة الأوروبية لمكافحة جرائم الإنترنت

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الإنترنت وسط انتقادات من دعاة حماية الحرية الشخصية وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الاتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب

بالبيـــانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي .

وتتضـــمن بـــنود المعاهدة التي تم تعديل مسودتها ٢٧ مرّة قبل الموافقة عليها فقـــرات تكفـــل للحكومـــات حق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلـــة وفـــرض القـــانون لكن الصلاحيات الدولية الجديدة ستكون على حساب حمايـــة المواطنين من إساءة الحكومات استخدام السلطات التي أعطتها لهم تلك الاتفاقية ة التي قد يسيئون استخدامها

٢ – إصـــدار قوانيـــن جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق

اتجهـــت كافـــة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجـــرم تلـــك الجرائم الإلكترونية MADE A NEW LAWS FOR THE ELECTRONIC CRIMES الجديـــدة على قوانينها التقليدية القديمة و عليه فقد صاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة و المتطورة تكنولوجيا ·

أ – على المستوى العالمي

تعتـــبر دولـــة الســـويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائـــم الإنترنت MADE A NEW LAWS FOR THE INTERNET CRIMES AND COMPUTERS CRIMES و الحاســـــب الآلى لتستطيع أن تعاقب المتهمين بأرتكاب تلك الجرائم الإلكترونية

TO CAN PUNISH THE DEFENDANTS WITH PERPETRATING THE ELECTRONIC CRIMES حيث صدر أول قانون خاص بها THE FIRST SPECIAL LAW سمي بقانون (البيانات) و قد صدر هذا القانون عام ١٩٧٣ م و قد عالج هذا القانون قضايا الاحتيال عن طريق الإنترنت بالإضافة إلى كونه يشتمل علي فقرات عامة من نصوصه لتشمل جرائم الدخول غير المشروع على البيانات الإلكترونية THE UNLEGAL ENTERING TO THE ELECTRONIC INFORMATION أو تزوير المعلومات الإلكترونية FORGING THE ELECTRONIC INFORMATION أو تحويلها أو الحصول غير المشروع عليها ٠

و كانت الولايات المتحدة الأمريكية هي الدولة التالية التي تبعت السويد في إصدار قوانين خاصة بها SPECIAL LAWS تجرم الجرائم الإلكترونية لحيث شرعت قانونا خاصا SPECIAL LAW بحماية أنظمة الحاسب الآلي (١٩٧٦ م – ١٩٨٥ م) و في عام ١٩٨٥ م حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية و هي : –

- جرائم الحاسب الآلي الداخلية
- جرائم الاستخدام غير المشروع عن بعد
- جرائم التلاعب بالحاسب الآلي
- دعم التعاملات الإجرامية
- سرقة البرامج الجاهزة و المكونات المادية للحاسب

و في عام ١٩٨٦ م صدر قانونا آخر يحمل الرقم ١٢١٣ عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الضرورية اللازمة لتطبيقه ٠

و علـــى اثـر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها علـــى حـده للـتعامل بها مع تلك الجرائم الإلكترونية ELECTRONIC CRIMES و مـن تلـك القوانيـن القـانون الخاص بولاية تكساس لجرائم الحاسب الآلي ٠

و قـد خولـت وزارة العدل الأمريكية في عام ٢٠٠٠ م خمس جهات حكوميـة للـتعامل مـــع جـرائـم الإنترنــت و الحاسب الآلي منها مكتب التحقيقات الفيدرالي F B I ٠

أمـا بريطانـيا فهي ثالـث دولة تسن قانون خاص بها SPECIAL LAW بجرائم الإنترنت حيـث أقرت قانون لمكافحة التزويـر و التزييف عام ١٩٨١ م الـذي شمل في تعاريفه الخاصة تعريف أداة التزوير DEFINITION OF FACILITY OF THE FORGING و وسـائط التخزيـن الحاسوبية المتـنوعة أو أي أداة أخرى يتم التسجيل عليها سـواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى ٠

أمـا كـندا فهـي تطبق قوانين متخصصة و مفصله للتعامل مع جرائم الإنترنت INTERNET CRIMES حيـث عدلت في عام ١٩٨٥ م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي و الإنترنـت كما شمل القانون الجديد أيضا تحديد للعقوبات المطبقة على المخالفات الحاسوبية و جرائم التدمير و جـرائم الدخـول غـير المشـروع علـى المعلومـات الإلكترونية THE UNLEGAL ENTERING TO THE ELECTRONIC INFORMATION كمـا وضح القانون صلاحيات جهات التحقيق كما جاء في قانون المنافسـة الذي يخول لمأمور الضبط القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي و التعامل معها و ضبطها ٠

أما الدانمارك فقد انتبهـت لهذا الأمر مبكرا أيضا فقد سنت أول قانون الخاص

THE FIRST SPECIAL LAW بهـا في مجال مكافحة جرائم الإنترنت STRIVING THE INTERNET CRIMES AND THE COMPUTERS CRIMES و الحاسـب الآلـي فـي عام ١٩٨٥ م و قد شـمل القـانون العقوبـات المحددة على ما يرتكب من جرائم مثل الدخول غير المشـروع إلـى الحاسب الآلي THE UNLEGAL ENTERING TO THE COMPUTERS أو تزويـر البـيانات FORGING THE ELECTRONIC DATA سواء كان هذا التزوير بالحذف أو بالإضافة أو بالتعديل ٠

أمـا فرنسا فهي من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجـرائم التكنولوجية الحديثة - جرائم الإنترنت INTERNET CRIMES - فقـد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصـدرت أول قانون خاص بها THE FIRST SPECIAL LAW في عام ١٩٨٨ م القـانون رقـم (١٩ - ٨٨) و الذي أضاف إلى قانون العقوبات الجنائـي جرائم الحاسب الآلي و العقوبات المقررة لتلك الجرائم كما تم في عام ١٩٩٤ م تعديـل قـانون العقوبـات لديها ليشمل مجموعة جديدة من القواعد القانونـية الخاصـة بالجرائم المعلوماتية و قد أوكل هذا القانون LAW إلى النـيابة العامـة سـلطة التحقيق فيها بما في ذلك طلب عمل التحريات و سماع الأقوال و الشهود ٠

أمـا هولـندا فقـد قامت هي أخرى بتعديل القوانين الخاصة بها للتوائم مع تلك الجـرائم الحديثة ليكون في إمكانها التعامل معها و محاولة السيطرة عليها فقد قامـت بتعديل القوانين الخاصة بها و نصت في تلكم القوانين على انه من حق القاضـي أن يصـدر أوامره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة و متى كان هذا التصنت على قدر عال من الأهمية للكشف

عن تلك الجريمة ٠

أمـــا فنلـــندا فهي الأخرى قد قامت بتعديل قوانينها الجنائية لتتسع لتلك الجرائم الإلكترونـــية الحديثة THE MODERN ELECTRONIC CRIMES و طبقا لتلك التعديلات فقد اصبح لمأمور الضبط القضائي الحق في التصنت على المكالمات الخاصة بشبكات الحاسب الآلي ٠

أمـــا فـــي ألمانيا فقد تم تعديل القوانين الخاصة بها و اصبح للقاضي الحق في إصدار أوامره بمراقبة اتصالات الحاسب الآلي و تسجيلها و التعامل معها إلا أن القانون قد أعطى ذلك المحقق بشرط إلا في مدة أقصاها ثلاثة أيام ٠

أمـــا فـــي الـــيابان فقد قامت هي الأخرى بسن القوانين الخاصة بها لتستوعب المســـتجدات الإجرامية المتمثلة في جرائم الإنترنت و الحاسب الآلي و قد نصت تلـــك القوانيـــن على انه لا يلزم مالك الحاسب الآلي OWNER OF THE COMPUTER المســـتخدم فـــي جـــريمة ما التعاون مع جهات التحقيق أو إفشاء كلمة السر DIVULGING THE PASSWORD التي يستخدمها إذا مـــا كـــان ذلك سيؤدى إلى أدانته كما أقرت في قانون خاص SPECIAL LAW ســـنته عام ١٩٩١ م شرعية التصنت على شبكات الحاسب الآلي فقط إذا مـــا كان ذلك في مجال البحث عن الأدلة الخاصة بإحدى الجرائم الإلكترونية THE EVIDENCE OF THE INTERNET CRIME ٠

وفـــي دولـــة المجر فقد قامت هي أخرى بسن قوانين خاصة بها لتجرم الجرائم الإلكترونـــية INTERNET CRIMES و قـــد نصـــت تلك القوانين التي سنتها على كيفيـــة التعامل مع مثل هذا النوع من الجرائم و أيضا كيفية التعامل مـــع المتهميـــن بارتكـــاب الجـــرائم DEFENDANTS WITH PERPETRATING THE CRIMES و هـــي الإجراءات التي تسهل عمل الجهات المنـــوط بها مواجهـــة مثل تلك الجرائم و القبض على المتهمين

بارتكابها ٠

أمـــا في دولة بولندا فهي أيضا سنت القوانين الخاصة بها و تلك القوانين التي سـنتها تنص على أن للمتهم بارتكاب الجرائم DEFENDANT WITH PERPETRATING THE CRIMES الحق في عدم طبع أي سجلات خاصـة بالحاسـب الآلـي أو إفشاء كلمات السر المستخدمة أو حتى ألا كواد الخاصـة بالـبرامج كمـا أنهـا تـنص علـى حقـوق أخرى بالنسبة للشهود WITNESSES فـي تلـك الجرائم فهي تعطى الشاهد WITNESS أيضا الحـق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك قد يؤدى إلى أدانته أو إدانة أي من أقاربه بل أن تلك القوانين تذهب إلى مدى ابعد من ذلك فتلك القوانين تنص على أن لا يقابل ذلك أي إجراء قسري قد يـتخذ و تكـون مـن نـتائجه إدانـة بالمتهم CONDEMNING THE DEFENDANT ٠

ب – على المستوى العربي

أمـا عن الحال في الدول العربية فانه للأسف لا توجد أي دولة عربية قد قامت بسـن قوانيـن جديـدة NEW LAWS خاصة بها أو حتى تحديث قوانينها MODERNISATION THE LAW الخاصة لتستوعب تلك المستجدات الإجرامـية فـالدول العربـية لا زالت بعيدة كل البعد عن ذلك التطور القانوني EVOLUTION OF LAWS الـذي يحـاول اللحاق بالتطور الإجرامي بينما نجد أن الدول العربية لا زالت لا تحرك ساكنا ٠

فمصـر على سبيل المثال لا الحصر لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال و لم تقم حتى بتعديل ما لديها من قوانين و إنما القانونيين في

مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية و التي تفرض نوعا من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة لأركان الجريمة المعلوماتية و من ذلك على سبيل المثال اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات كما تم تطويـــع نصـــوص قـــانون حماية الحياة الخاصة و قانون تجريم إفشاء الأسرار بحيـــث يمكن تطبيقها على بعض جرائم الإنترنت INTERNET CRIMES و أوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية ٠

و علـــيه فان وجد نص قانوني يعاقب على جريمة شبيهة بالجريمة المعلوماتية يـــتم أدراجها تحته و تتقرر العقوبة المنصوص عليها في ذلك النص و عليه و دائمـــا و فـــي جمـــيع الأحوال لا تكون العقوبة المنصوص عليها في هذا النص القانونـــي تتناســـب و حجـــم الخســـائر النـــتائج عن ارتكاب مثل تلك الجريمة الإلكترونـــية و لأنه لا يوجد نص صريح CANDID TEXT خاص بها و يعاقـــب علـــيها و يعطى العقوبة المناسبة للأضرار الناتجة من تلك الجريمة يتم أدراج تلـــك الجـــريمة المعلوماتـــية تحت هذا النص القانوني LAW TEXT الغـــير خـــاص بهـــا و الموضوع للعقاب على جريمة أخرى و بالتالي لا يكون العقاب المنصوص عليه مناسب ٠

أمـــا في المملكة العربية السعودية فهي لا تواجه نفس تلك المشاكل على أساس أن كافـــة تشـــريعاتها LAWS تنطلق من الشريعة الإسلامية و بالتالي فهي لا تحـــتاج إلـــى تحديـــث فالشـــريعة الإسلامية لا تحتاج إلى أي تحديث فالشريعة الإسلامية صالحة لكل زمان و مكان ٠

وقـــد اتخـــذت مدينة الملك عبد العزيز للعلوم و التقنية من خلال وحدة الإنترنت المشرفـــة على عمل مقدمي خدمة الإنترنت INTERNET في المملكة عدد

من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين و المتسللين و منعهم و قد أوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين و إساءة استخدام البريد الإلكتروني E _ MAIL و غيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الإنترنت في المملكة و من بين هذه الإجراءات ما يأتي : -

- ١ - منع انتحال أرقام الإنترنت أو ما يعرف بـ (IP-SPOOFING) و التي يقوم من خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة .
- ٢ - العمل على منع إساءة استعمال البريد الإلكتروني أو ما يعرف بـ (E _ MAIL SPAMMING) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا بأسم البريد المهمل و الذي ينتشر بشكل كبير في الدول المتقدمة .
- ٣ - DIALUP - SERVER أي الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين و سجل استخدام البروكسى PROXY لمدة لا تقل عن ستة اشهر .
- ٤ - الحصول على خدمة الوقت LTP عن طريق وحدة البروكسى و مزود الاتصال بهدف اللجؤ إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات .
- ٥ - تحديث سجلات منظمة رايب WWW . RIPE . COM الخاصة بمقدمة الخدمة .
- ٦ - ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة و معاقبة المخالفات الأمنية .

٣ – التعاون الدولي

مـــن المعـــروف أن جـــرائم الإنترنت هي جرائم عابرة للحدود أي أنها لا تتم و تنتهـــي فـــي أراضـــي دولـــة بعينها و عليه فالتعاون ألد ولى هو من أهم سبل مكافحـــة جـــرائم الإنترنت و ملاحقة مرتكبيها فبغير التعاون الدولي يزداد معدل ارتكـــاب تلك الجرائم و يطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من الســـهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها ما ارتكبوه من جرائم ٠

و تعتـــبر المعاهدات الدولية التي تنضم إليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي في ذلك المجال ٠

و مـــثال ذلـــك أيضا التعاون الدولي في مجال مكافحة الجريمة المنظمة و قد بدا هـــذا الـــتعاون الدولي بمؤتمر الأمم المتحدة السابع و الذي عقد عام ١٩٨٥ م امـــنع الجـــريمة المـــنظمة حيـــث اعتمد خطة عمل ميلانو و التي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة و القضاء عليها ٠

و تبع ذلك الاجتماع الإقليمي التحضيري و الذي عقد عام ١٩٨٨ م و الذي تم فـــيه إقـــرار المبادئ التوجيهية لمنع الجريمة المنظمة و مكافحتها ثم المؤتمر الثامـــن لمنع الجريمة بفنزويلا عام ١٩٩٠ م فالمؤتمر الوزاري العالمي المعنى بالجـــريمة المنظمة عبر الوطنية في نابولي بإيطاليا عام ١٩٩٤ م و الذي عبر عـــن إرادة المجـــتمع الدولي بتعزيز التعاون الدولي و إعطاؤه الأولوية لمكافحة الجريمة المنظمة ٠

و كانـــت معاهدة المجلس الأوروبي حول جرائم الشبكات الإلكترونية التي أيدتها الولايـــات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعملية وضـــع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها

في نهاية الأمر في جهودها التشريعية والتنظيمية وتطبيق القوانين .

و يستند نهج هـــــذه المعاهدة إلى اعتراف أساسي بضرورة قيام انسجام بين قوانيـن الـدول المعنية و قد تم تحقيق التعاون الدولي في تطبيق القوانين من خـلال سلسـلة مـن معـاهدات تسليـم المجرمين والمساعدة القانونيـة المتـبادلة (MLAT) التي تمكن الحكومات من تبادل المعلومات والأدلة وبغية وضـع هذه المعاهدات قيد التنفيذ يفترض عادة وجود ما يعرف بازدواج العمل الإجرامي (أي ان تكون السلطات القضائية لكلا الدولتين تعتبر ذلك العمل عملاً جرمـياً) و عليه يتم تسهيل التعاون الدولي بدرجة كبيرة من خلال التلاقي على مـا يمكـن اعتباره عملا إجرامياً بموجب تشريعات مختلف البلدان المعنية فان فرض قوانين مماثلة في مختلف الدول يزيد المخاطر التي تواجه مرتكبي جرائم الإنترنـت ويتجه اكثر نحو معادلة هذه المخاطر في مختلف الدول المعنية وفي الواقـع كلمـا كانت القوانين أكثر شمولاً كلما قلت الملاذات الآمنة التي يستطيع المعتدون على الشبكات الإلكترونية العمل انطلاقاً منها بأمان .

ان الانســجام ضروري بالنسبة إلى القوانين الأساسية كما بالنسبة إلى القوانين الإجرائـية و على كافة الدول ان تُعيد تقييم ومراجعة قواعد الإثبات و التفتيش وإلقـاء القـبض والتنصت الإلكتروني وما شابه ذلك لتشمل المعلومات الرقمية وأنظمـة الكمبيوتر الحديثة وأنظمة الاتصالات الحديثة والطبيعة العالمية لشبكة الإنترنـت أمـا التنسيق الأكبر للقوانين الإجرائية فيمكن أن يُسهّل التعاون في التحقيقات التي تشمل سلطات قطاعية متعددة .

بالإضـافة إلـى القوانيـن الملائمة من المهم أيضاً ان تطور الحكومات وأجهزة تطبيق القانون قدراتها على تطبيق هذه القوانين يحتاج ذلك إلى تطوير الخبرات في مجال الجريمة التي ترتكب عبر الشبكات الإلكترونية وتحقيق مشاركة فعالة

للمعلومـــات بين الدوائر داخل الدولة المعنية وبين مختلف الدول يضاف إلى ذلك ضـــرورة تخطـــي هذه المشاركة الأجهزة التقليدية لتطبيق القوانين بحيث تشمل أجهـــزة الأمن القومي وأجهزة الاستخبارات كما ان من الأمور الأساسية تشكيل وحـــدات متخصصة في تطبيق القانون للتعامل مع المسائل المتعلقة بهذا النوع من الجرائم على مستوى البلد المعني بإمكان هذه الوحدات أيضاً ان توفر أساساً للـــتعاون الدولـــي الرسمي وغير الرسمي المستند إلى شبكات ثقة بين مسؤولي تطبـــيق القوانين في مختلف البلدان ويمكن للتعاون في قضية معينة أو التعاون فـــي لجـــان مشتركة مؤلفة من ممثلي عدد من الدول أن يكون مفيداً جداً وهناك قضـــايا كـــان فـــيها التعاون الدولي فعالاً للغاية وبالفعل يمكن ان يولد التعاون الناجح تعاوناً مماثلاً في أماكن أخرى ويحقق المزيد من النجاح .

و علـــي مستوي العالم العربي وضعت لجمة مكافحة الجرائم المنظمة مقترحات للعمـــل العربـــي في مكافحة الإرهاب و التي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة و في عام ١٩٩٦ م وافق المجلس في دورته الثالثة عشـــر علـــى مدونة سلوك طواعية لمكافحة الإرهاب ووافق عام ١٩٩٧ م في دورته الرابعة عشر على استراتيجية عربية لمكافحة إرهاب وفي عام ١٩٩٨ م اقر مجلس وزراء الداخلية و العدل العرب الاتفاقية العربية لمكافحة الإرهاب ٠ هـــذا فـــي مجال مكافحة الجرائم المنظمة أما في مجال التعاون الدولي لمكافحة الاتجـــار فـــي المخـــدرات فقد اهتمت كافة الدول بهذا الموضوع لما يسببه من أضـــرار على اقتصادياتها و كذلك لما يسببه من إنهاك لثروتها البشرية و التي تعتمد عليها أي دولى في تحقيق تقدمها الاقتصادي و عليه فقد كان هناك تعاونا دولـــيا قويـــا في مجال مكافحة الاتجار في المخدرات و مساعدة المدمنين على الإقلاع عن الإدمان ٠

وقـــد عقدت اتفاقية مكافحة المخدرات عام ١٩٦١ م و اتفاقية المؤثرات العقلية عـــام ١٩٧١ م و اتفاقـــية الأمـــم المـــتحدة لمكافحـــة الاتجار في المخدرات و المؤثرات العقلية عام ١٩٨٨ م ٠

و علـــى المســـتوى العربـــي تـــم عام ١٩٩٦ م إقرار الاتفاقية العربية لمكافحة الاتجـــار فـــي المخـــدرات و المؤثـــرات العقلية كما تم في عام ١٩٩٦ م إقرار القانون العربي النموذجي الموحد للمخدرات

و علـــيه فإنـــه لتفعـــيل التعاون الدولي لابد من التركيز على ثلاث موضوعات رئيسية لابد من العمل على تعظيم وجودها و الأخذ بها وهي كالآتي : -

- ١ – الانضـــمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون و التنسـيق بيـــن الجهـــود التـــي تبذلها الدول في مجال مكافحة جرائم الإنترنت

- ٢ – إدخـــال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي أي تنفيذ ما تنص عليه تلك الاتفاقيات من إجراءات دون أي إبطاء

- ٣ – العمل على وجود اكبر قدر ممكن من التناسق و التطابق فيما بين قوانيـــن الـــدول المختلفة و المتعلقة بمكافحة جرائم الإنترنت فلا يكون الفعـــل الذي تم ارتكابه جريمة في بلد ما و غير معاقب عليه في قانون بلـــد آخـــر فمن هنا يجد المجرمون الملاذ الأمن الذي يلجئون إليه دون أي اعتبار لما ارتكبوه من جرائم ٠

- ٤ – تعـــاون جمـــيع الـــدول في تسليم المطلوبين أمنيا إلى الدول التي تطالب بهم لارتكابهم جرائم الإنترنت ٠

٤ – اتحاد الشركات و الكيانات الاقتصادية في مجال حماية أمنها الإلكتروني

تعد الكيانات الاقتصادية من أهم الأهداف المحتملة لأي عمليات إجرامية تتم عبر الإنترنت و غالبا ما يكون الهدف من ارتكاب تلك الجرائم هو البحث عن أموال تلك الشركات الضخمة أو عما تخفيه من معلومات تريد الشركات الأخرى الحصول عليها في محاولة منها للتغلب على ما تعانيه من نقص في المعلومات التكنولوجية التي تساعدها على النهوض تكنولوجيا و تصبح في عداد الشركات الاقتصادية الكبرى و المتقدمة اقتصاديا بما يعود عليها من فوائد اقتصادية ضخمة و عليه فغالبا ما تكون الشركات الاقتصادية هي الهدف السمين الذي يلهث وراءه مرتكبي جرائم الإنترنت ٠

أيضا قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة هي الحصول على معلومات هامة عنها للقيام بابتزازها و الحصول منها على مبالغ مالية في مقابل عدم نشر ما تم الاستيلاء عليه من معلومات في الغالب يكون نشرها ضارا بالشركة ضررا بالغا ٠

و عليه فأن الكثير من الكيانات الاقتصادية الهامة في العالم تتحد مع بعضها البعض في محاولة منها للقيام ببناء حائط صد إلكتروني مضاد لما قد تتعرض له من هجمات و محاولات اختراق و قرصنه من محترفي ارتكاب جرائم الإنترنت و مكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها البعض في هذا الأمر ٠

- ١ – فمن ناحية فأن التعاون الذي يتم بينها و بين الكيانات الاقتصادية الأخرى يوفر لها قدرا كبيرا من الأموال فيما لو كانت ستقوم ببناء هذا

- الحـــائط المضـــاد بمفردها فعندها كانت ستتحمل بمفردها ما يتكلفه من أموال دون أي مساعدة من أي جهة خارجية
- ٢ - و مـــن ناحية أخرى فأن هذا الاتحاد يكون ائتلافا قويا في مواجهة تلـــك الهجمـــات التتارية على تلك الكيانات و بالتالي يجعلها أقوى عند مواجهة تلك الاختراقات و صدها و تعقب مرتكبيها ·
- ٣ - أن تعـــاون تلـــك الشركات و عدم تحمل أي منها للتكاليف بمفرده يجعلها تستطيع القيام ببناء حائط صد قوى و منيع في مواجهة مرتكبي جـــرائم الإنترنت و بالتالي يصعب كثيرا من فرص اختراقه و النفاذ إلى تلك الشركات ·

و علـــيه نجـــد أن تعـــاون الكيانات الاقتصادية الكبرى في مجال مكافحة جرائم الإنترنـــت يســـاعد كثيرا على حماية امنها من مخاطر التعرض لتلك الجرائم و يحـــافظ عليها من أي محاولات ابتزاز قد تتعرض لها إذا ما استطاع أي شخص الـــنفاذ إلى معلوماتها أو الحصول عليها فعندئذ سيكون عليها أن تدفع له الكثير من الأموال لمنعه من نشر معلوماتها السرية و التي قد تستفيد منها أي شركات منافسه لها في الأسواق العالمية أو التي قد تضر بالشركة ضررا بليغا إذا ما تم نشر تلك المعلومات ·

٥ - المعاهدات و القوانين الخاصة بحماية حق الملكية الفكرية

و تعتـــبر حمايـــة الملكية الفكرية هي من اكثر الحقوق التي يتم انتهاكها يوميا علـــى شبكة الإنترنت او على كافة شبكات الاتصالات و المعلومات على مستوى العـــالم و علـــيه فوجود معاهدات دولية تمنع تلك الانتهاكات و إصدار كل دولة قوانين خاصة بها تعمل على حمايـــــة حقوق الملكية الفكرية كل ذلك يؤدى إلى

الحفـــاظ علـــى تلـــك الحقوق من الانتهاك الذي يتم يوميا دون أي رادع يحمى أصحاب تلك الحقوق ٠

و سوف نعرض أولا للمعاهدات التي تم إبرامها في هذا المجال و سوف نعرض ثانـــيا لمـــا تـــم إصداره من قوانين في هذا المجال و لكن عرضنا سيكون على مســـتوى الـــدول العربية في محاولة لمعرفة مدى تقدمنا الثقافي الذي أصبحت الكثـــير مـــن الأمم المتقدمة تقيسه ما تقدمه الدولة من حماية في مجال حماية حقوق الملكية الفكرية ٠

أولا : - المعـــاهدات الدولـــية التي تم إبرامها في مجال حماية حقوق الملكية الفكرية

مـــن أهـــم المعـــاهدات التي تم إبرامها في هذا المجال معاهدات ثلاث هم على التوالي : -

- ١ - معاهدة برن
- ٢ - معاشدة تريبس
- ٣ - معاهدات الويبو

١ - معاهدة برن لحماية المصنفات الأدبية و الفنية

تعتـــبر معـــاهدة برن و التي تم التوقيع عليها في عام ١٩٧١ في سويسرا هي حجـــر الأســـاس فـــي مجال الحماية الدولية لحق المؤلف و قد وقعت على هذه الاتفاقية ١٢٠ دولة من بينها جمهورية مصر العربية و تعد المادة التاسعة من

تلــك الاتفاقية هي أساس في تلك الاتفاقية لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة و بأي شكل كان ٠

وفضلا عن ذلك تمنح اتفاقية برن صاحب حق المؤلف الحق في أن يرخص أو يمــنــــع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أم أجنبيا

٢ - معاهدة تريبس

الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية

معــاهدة تريــبس هــي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الإلكتروني على العمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية ٠

و تلــك الاتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام ١٩٩٤ و قد عــالج موقعــو الاتفاقــية العامة للتعريفات و التجارة (الجات) حقوق الملكية الفكريــــة بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية T R I P S فربطوا بذلك بين المعايير الدولية و المعايير المحلية و تتضمن تلك الاتفاقــية العديد من الإجراءات الهامة و الفعالـــة لردع الاعتداءات على حقوق الملكــية الفكرية كما أنها و من جهة أخرى تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع و من تلــك التدابير على سبيل المثال لا الحصر إعطــاء الحــق للسلطات في إصــدار الأوامر بشن حملات مفاجئة لضبط أدلة

ارتكــاب الجــريمة و التــي عادة ما تكون سهلة التخلص منها لو لم تكن هناك ســرعة فــي محاولة ضبطها و كذلك التحفظ على أدوات ارتكاب الجرائم و ذلك فضلا عن فرض عقوبات جنائية رادعة .

و فــي حالة تراخي الدولة العضو عن اتخاذ مثل تلك الإجراءات أو أن تهما في تطبــيق قوانيــنها الوطنية فأن المنظمة العالمية تعلن أن تلك الدولة لا تقوم بما علــيها مــن واجــبات فــي تطبيق الشروط و الإجراءات المنصوص عليها في المعــاهدة و بالتالي تكون عرضة لان تتخذ ضدها العديد من الإجراءات العقابية من باقي الدول الأعضاء .

٣ – معاهدات الويبو

في البداية نوضح أن معاهدة الويبو تنقسم إلى ثلاث معاهدات هي : –

- معاهدة الويبو بشأن حق المؤلف
- معاهدة الويبو بشأن الأداء و التسجيل الصوتي
- معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة

١ – معاهدة الويبو بشأن حق المؤلف

تــم التوقيع على تلك المعاهدة في ٢٠ ديسمبر عام ١٩٩٦ و تتكون من ثمانية عشــر مــادة و تــبدأ بالديباجة ثم تتناول علاقة تلك المعاهدة بمعاهدة برن ثم تــتعرض لــنطاق تطبــيق حمايــة حق المؤلف كحق التوزيع و التأجير و نقل المصنف إلى الجمهور و الالتزامات المتعلقة بالتدابير التكنولوجية و الالتزامات المــتعلقة بالمعلومــات الضرورية المتعلقة بالحقوق و مدة حماية المصنفات و الإستثناءات و التقييدات على تلــك الحقوق و كذلــك الحقوق و الالتزامات

المترتـبة على المعاهدة و دخول المعاهدة حيز التنفيذ الفعلي و أخيرا تعرضت المعـاهدة للتحفظ عليها و نقضها سواء من قبل أحد أطرافها الموقعين عليها أو من إحدى الدول الغير موقعة عليها و لغاتها ٠

و تـنص الجملـة الأولـى من المادة الأولى من المعاهدة الأولى على أن هذه المعـاهدة اتفـاق خـاص بمعنى المادة ٢٠ من اتفاقية برن لحماية المصنفات الأدبـية والفنية بالنسبة إلى الأطراف المتعاقدة من بلدان الاتحاد المنشأ بموجب تلك الاتفاقية .

وتـنص المادة ٢٠ من اتفاقية برن على أن تحتفظ حكومات دول الاتحاد بالحق فـي عقـد اتفاقات خاصـة فيما بينها ما دامـت هـذه الاتفاقات تخول حقوقا تفوق تلك التي تمنحها هذه الاتفاقية أو تتضمـن نصوصا لا تتعارض مع هذه الاتفاقيـة ٠

وكانت للنص السالف الذكر من للمادة الأولى من المعاهدة الأولى بالتالي أهمية خاصـة في تفسير المعاهدة إذ أنه يبين أن تفسير المعاهدة الذي قد يؤدي إلى الحد من الحماية التي تمنحها اتفاقية برن يعتبر مرفوضا .

وتعطـي المادة الرابعة من المعاهدة الأولى ضمانا إضافيا للالتزام باتفاقية برن بأكـبر قـدر ممكن إذ أنها تضم جميع الأحكام الجوهرية لاتفاقية برن بالإحالة إليها وتنص على أن (على الأطراف المتعاقدة أن تراعي المواد من ١ إلى ٢١ والملحق من اتفاقية برن)

وتوضـح المادة الثالثة أن اتفاقية برن تشير في ذلك السياق إلى وثيقة باريس لاتفاقية برن لسنة ١٩٧١

وينبغي قراءة تلـك النصوص على ضوء أحكام المادة ١٧ من المعاهدة التي

سنناقشـها لاحقـا وبـناء علـى تلك المادة لا تكون المعاهدة متاحة للبلدان الأطـراف فـي وثيقة باريس لسنة ١٩٧١ والبلدان الأطراف في أية وثيقة من وثائق اتفاقية برن فحسب بل بالنسبة أيضا إلى كل دولة عضو في الويبو سواء كانـت طرفا في الاتفاقية أو لم تكن طرفا فيها ويجوز لبعض المنظمات الدولية الحكومية أيضا أن تصبح أطرافا في المعاهدة .

وتحـتوي المادة الثانية من المعاهدة الأولى بند ضمان مشابها للبند الوارد في المـادة ٢-٢ من اتفاق تريبس وتنص على أنه ليس في هذه المعاهدة ما يحد من الالتزامات المترتبة حاليا على الأطراف المتعاقدة بعضها تجاه البعض الآخر بناء على اتفاقية برن لحماية المصنفات الأدبية والفنية غير أن نطاق ذلك البند يخـتلف عن نطاق البند الوارد في اتفاق تريبس وينطوي الأخير على أهمية من وجهـة نظـر مادة واحدة على الأقل من اتفاقية برن تضم أحكاما جوهرية أي المـادة السادسة المتعلقة بالحقوق المعنوية إذ لا ينص اتفاق تريبس على أية حقوق أو التزامات فيما يتعلق بتلك المادة

٢ – معاهدة الويبو بشأن الأداء و التسجيل الصوتي

تـم التوقيع على تلك المعاهدة في ٢٠ ديسمبر ١٩٩٦ و تقع تلك المعاهدة في أربـع فصـول يتـناول الفصل الأول منها الأحكام العامة ة علاقة تلك المعاهدة بالمعـاهدات و الاتفاقات الدولية الأخرى و التعريف و المستفيدون من الحماية بناء على تلك المعاهدة و كذلك المعاملة الوطنية .

أما الفصل الثاني فيتناول حقوق فناني الأداء معنويا و ماليا و حقوق الاستنساخ و التوزيع و التأجير و حق إتاحة الأداء المثبت .

أما الفصل الثالث فيتناول حقوق المنتجين كحق الاستنساخ و التأجير و التوزيع

و حق إتاحة التسجيلات الصوتية ،

و يتناول الفصل الرابع الأحكام المشتركة فيتناول الحق في مكافأة مقابل الإذاعة أو النقل إلى الجمهور و التقييدات و الإستثناءات على هذا الحق و مدة الحماية و الالتزامات المتعلقة بالتدابير التكنولوجية و الالتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق و أخيرا تم التعرض للإجراءات الشكلية ،

٣ - معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة

و تبدأ تلك الاتفاقية بمقدمة ثم تتناول الطابع القانوني للمعاهدتين الجديدتين و علاقتهما بالمعاهدات الدولية الأخرى ثم تتناول الاتفاقية جدول الأعمال الرقمي و المعاهدات الجديدة ثم تتعرض الاتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديدتين و أخيرا أعمال المتابعة بعد المؤتمر الديبلوماسي ،

ثانيا : - القوانين التي أصدرتها الدول العربية في مجال حماية حقوق الملكية الفكرية

أما بالنسبة لقوانين حماية الملكية الفكرية التي تم إصدارها فسوف نعرض لتلك القوانين التي صدرت على مستوى عالمنا العربي

١ - قانون حماية الملكية الفكرية الصادر بدولة الإمارات العربية المتحدة

وضعت دولة الإمارات العربية المتحدة في العام ١٩٩٢ قانوناً لحماية الملكية الفكرية بموجب القانون الاتحادي رقم (٤٠). وتشمل المواد التي تضمنها قانون

حقـوق الملكـية الفكرية برامج الكمبيوتر بالتحديد. وبالتالي يصبح نسخ المواد المحمـية بموجـب قانون حماية الملكية الفكرية من غير إذن أو توزيع نُسخها عمـلاً غـير قانوني . فلا يجوز صنع أية نسخ من غير إذن صريح من صاحب حق الملكية الفكرية

يمـنع قانون دولة الإمارات العربية المتحدة نسخ برامج الكمبيوتر بـدون إذن وكـل مـن يقبض عليه متلبساً بقرصنة البرامج سيخضع هو وشركته للمحاكمة بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب القانون غرامة مالية قدرهـا ٥٠٠٠٠ درهماً أو أكثر بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل إلى ثلاث سنوات

مسـؤوليات المسـتخدم : - إن أولى مسؤولياتك كمستخدم لبرامـج الكمبيوتر هـي أن تشـتري البرامـج الأصلية وإذا اشتريت البرامـج لاستخدامها في أعمـالك الـتجارية ينبغـي أن يكون لكل جهاز كمبيوتر في شركتـك مجموعته الخاصة من البرامج الأصلية

ولهذا ينبغي عليك أن تتأكد عند شراء برامـج كمبيوتر من أن المنتجات التي تشتريها قانونية ذلك أن العديد مـن المنتجات المزوّرة تكون أحيانا مصممة بشـكل تبدو فيه مشابهة لمنتجات الصانع الأصلي إلا أنها تكون متدنية الجودة وبالتالـي فـإن مشـتري ومستخدمي البرامج المزوّرة أو المنسوخة يواجهون مجازفات لا مبرر لها تتمثل في : -

- ١ - الفيروسات أو الأقراص التالفة أو البرامج ذات العيوب الأخرى

- ٢ - عـدم وجـود المسـتندات الضـرورية التي تمكنك من استخدام البرنامج بشكل صحيح

- ٣ - عـدم حصـولك على الدعم التقني للمنتجات المتوفر للمستخدمين المسجلين

- ٤ - عـدم حصـولك علـى الـبرامج المطـورة التـي يحصل عليها المستخدمون المسجلون

- ٥ - وبالإضافة إلى ذلك فأن شراء البرامج الأصلية يعنى أن جزأ كبيرا مـن هـذا الثمـن سوف يخصص إلى برامج التطوير إلى تعنى بتقديم الجديـد مـن الـبرامج الأسـهل و الأكثر تطورا بما يؤدى إلى تطور المنـتجات و تحديـثها و يـؤدى إلـى اللحـاق بركب الدول المتقدمة تكنولوجـيا هذا في حال شراء برامج أصلية أما عند شراء برامج غير أصـلية فـلا يكـون هناك أي مخصصات لبرامج التطوير و تذهب تلك النقود إلى القراصنة الذين نسخوا تلك البرامج دون أن يبذلوا أي جهد فـي إنـتاجها و دون أن يكون للشركات التي طورت و بحثت و أنتجت تلك البرامج أي نصيب من هذا الثمن مما يحرمها من الحصول عليه و بالتالي تقل الأموال التي يمكن إنفاقها على البحث و التطوير

و لقـد اتخـذت دولة الإمارات العربية المتحدة تدابير فعالة جداً لحماية حقوق الملكـية الفكـريةفقد نصت على عقوبات عديدة رادعة و قامت بحملات مداهمة عديـدة مـن خلالها تم القبض على كم كبير جدا من البرامج الغير أصلية وإنّ حمـــلات المداهمـة هذه ضدّ قراصنة برامج الكمبيوتر مستمرة لتشجيع شراء

البرامج الأصلية.

٢ - قـانون حمايـة الملكـية الفكرية الصادر بالمملكة العربية السعودية

يوفر نظام حماية حقوق المؤلف لمصنفات الحاسب الآلي الحماية لمدة خمسون عاما من تاريخ وفاة المؤلف أو من تاريخ النشر إذا كان المؤلف شخصا معنويا ويحظـر القـانون أي تقليد أو بيع أو إيجار أو توزيع أو استيراد أو تصدير أي مصنف دون إذن من مالك الحق .

الحقوق التي يتمتع بها المؤلف : -

بموجب هذا القانون يتمتع المؤلف بالحقوق الآتية : -

- ١ - استغلال مصنفه ماليا بأي طريقة من طرق الاستغلال المشروعة
- ٢ - نسـبة مصـنفه إلي نفسه ودفع أي اعتداء علي حقه وله كذلك الاعتراض علي كل تحريف أو تشويه أو تعديل أو تغيير لمصنفة أو كل مساس آخر بذات المصنف يكون ضارا بشرفة أو بسمعته
- ٣ - نشر مصنفة أو تسجيله أو عرضة أو نقله أو ترجمته و تقرير ما يتعلق بذلك من شروط وقيود
- ٤ - إدخال ما يراه من تعديل أو إجراء أو حذف على مصنفه
- ٥ - سحب مصنفه من التداول

العقوبات التي قررها القانون

- ١ - يعاقـب المعـتدى علي حق المؤلف بغرامة عشرة آلاف ريال أو بإغلاق المؤسسة أو المطبعـة التي اشتركت في الاعتداء أو بهما معا

- ٢ - بالإضافة إلي تعويض صاحب الحق عما لحقه من أضرار
- ٣ - في حالة العود يعاقب المعتدي بمضاعفة العقوبة السابق ذكره

٣ - قانون حماية الملكية الفكرية الصادر بدولة الكويت

أصدرت دولة الكويت القانون رقم ٩٩/٦٤ بشأن حماية حقوق الملكية الفكرية الذي يحمي برامج الكمبيوتر تحديداً وبموجب هذا القانون يعتبر نسخ المواد المتمتعة بحقوق الملكية الفكرية أو توزيع أو تأجير أو استيراد تلك النسخ بدون إذن من صاحبها عملاً غير قانوني فلا يجوز النسخ من غير إذن صريح من صاحب حق الملكية الفكرية إلا نسخة واحدة فقط لغرض المساندة.

العقوبات المقررة بموجب هذا القانون : - يمنع القانون الكويتي رقم ٩٩/٦٤ نسخ البرامج من غير إذن صاحب الحق وكل من يقبض عليه متلبساً بقرصنة البرامج سيخضع هو وشركته للمحاكمة وتشمل العقوبات حسب القانون غرامة مالية تصل إلى ٥٠٠ دينار كويتي أو الحبس لمدة قد تصل إلى سنة واحدة أو العقوبتين معاً وكذلك مصادرة المنتجات والتجهيزات المستخدمة في نسخ البرامج المزورة و إتلافها ونشر الحكم الصادر في المخالفة في وسائل الإعلام وعلى حساب المخالف وفي حال تكرار المخالفة خلال خمس سنوات من تاريخ الحكم السابق سوف تزداد العقوبة عن الحد الأقصى المقرر بما في ذلك إغلاق المنشأة لمدة قد تصل إلى ستة أشهر .

مسؤليات المستخدم المنصوص عليها في القانون : - إن أولى مسؤولياتك كمستخدم لبرامج الكمبيوتر هي أن تشتري البرامج الأصلية وإذا اشتريت البرامج لاستخدامها في أعمالك التجارية ينبغي أن يكون لكل جهاز كمبيوتر في

شركتك مجموعته الخاصة من البرامج والوثائق المرفقة بها .

ولهـذا ينبغـي عليك أن تتأكد عند شراء برامج كمبيوتر من أن المنتجات التي تشتريها قانونية ذلك أن العديد من المنتجات المزوّرة تكون أحياناً مصممة بشكل تـبدو فـيه مشـابهة لمنـتجات الصانع الأصلي، إلا أنها تكون متدنية الجودة وبالتالـي فـإن مشـتري ومستخدِمي البرامج المزوّرة أو المنسوخة يواجهون مجازفات لا مبرر لها :

- ١ - الفيروسات أو الأقراص التالفة أو البرامج ذات العيوب الأخرى

- ٢ - عـدم وجـود المسـتندات الضـرورية التي تمكنك من استخدام البرنامج بشكل صحيح

- ٣ - عـدم حصـولك على الدعم التقني للمنتجات المتوفر للمستخدِمين المسجلين

- ٤ - عـدم حصـولك علـى الـبرامج المطـورة التـي يحصل عليها المسـتخدِمون المسجلون

- وبالإضـافة إلى ذلك فأن شراء البرامج الأصلية يعنى أن جزأ كبيرا من هـذا الثمن سوف يخصص إلى برامج التطوير إلى تعنى بتقديم الجديد مـن الـبرامج الأسهل و الأكثر تطورا بما يؤدى إلى تطور المنتجات و تحديـثها و يؤدى إلى اللحاق بركب الدول المتقدمة تكنولوجيا هذا في حـال شـراء برامج أصلية أما عند شراء برامج غير أصلية فلا يكون هناك أي مخصصات لبرامج التطوير و تذهب تلك النقود إلى القراصنة

- الذين نسخوا تلك البرامج دون أن يبذلوا أي جهد في إنتاجها و دون أن يكــون للشركات التي طورت و بحثت و أنتجت تلك البرامج أي نصيب مــن هــذا الثمن مما يحرمها من الحصول عليه و بالتالي تقل الأموال التي يمكن إنفاقها على البحث و التطوير

لقــد التزمــت الحكومــة الكويتية بحماية حقوق الملكية الفكرية وتقوم بحملات مداهمة مفاجئة على القرصنة وفرض عقوبات رادعة على المخالفين تهدف إلى تشجيع إنتاج وشراء البرامج الأصلية .

الفصل الرابع

تجـربة جمهورية مصر العربية في مكافحة جرائم الحاسبات و شبكات المعلومات

للحديث عن تجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت أو ما يطلق عليه الجرائم المعلوماتية لابد أن يكون بداية الحديث عن تلك القوانين التــي لابــد و أن تكون موجودة كأساس يتم بموجبه تحديد ماهية الأفعال التي تعتــبر جرائم ففي كل الدول الحديثة المتقدمة تكنولوجيا و علميا و قانونيا يوجد قــانون للعقوبــات يحــدد الجرائم التقليدية و أركانها كل انه يوجد أيضا قانون الإجــراءات الجنائــية و هــو القانون الذي يقرر أساليب و وسائل الإبلاغ عن الجــريمة التقليدية و الطرق المتبعة في التحري عن صحتها و مرتكبيها و جمع الاستدلالات عنها و ضبطها و التحقيق فيها ثم أخيرا إحالة المتهم بارتكابها إلى المحاكمــة حيث تتم أدانته و يلقى العقاب المنصوص عليه في القانون جزاء ما ارتكبت يداه أو يقضى ببراءته فيطلق سراحه •

كــل ذلــك يستلزم وجود الدليل المقبول قضائيا لإدانة ذلك المتهم و من القواعد الثابتة في قانون العقوبات في أي دولة

- انه لا جريمة إلا بنص
- لا عقوبة إلا بقانون
- أن الشك يفسر لصالح المتهم

و علــيه فبعض الجرائم قد تتم بالأسلوب التقليدي العادي غير الإلكتروني فتقه تحــت طائلــة نصوص القانون السارية في الدولة و يلقي المتهم عقابه على ما ارتكبت يداه •

أما جرائم الاعتداء على نظم و شبكات المعلومات و شبكات الاتصال و التي تقع بالشكل الإلكتروني غير التقليدي لا تتوافر لها حتى الآن نصوص قانونية سواء

فـــي قانون العقوبات أو في قانون الإجراءات الجنائية لتجريمها و لتقرر العقوبة المقررة على كل جريمة تتم بهذا الشكل غير التقليدي ٠

هــذا مــن جهة و من جهة أخرى فأن تلك الجرائم الإلكترونية تشمل في معظم الأحــوال أفعالا ضارة تقع على نظم المعلومات و شبكات الاتصال و هو ما يؤثر بالســلب على التجارة الإلكترونية أو أي أعمال إلكترونية أخرى نظرا لان تلك الجــرائم تكون أداة الجريمة فيها نظم الحاسبات و البرمجيات و من ثم فانه لكي تــتوافر إمكانــية تجريــن تلك الأفعال و وضع العقاب على من يرتكبها لابد من توافــر نصــوص قانونية في قانون العقوبات و قانون الإجراءات الجنائية تجرم أفعــال الاعــتداء علــى نظم و شبكات المعلومات و الحاسبات و الاتصالات أي جــرائم المجال الإلكتروني أو ما يطلق عليه جرائم الإنترنت أو أي أفعال اعتداء علــى الأشخاص و الأموال و التي تقع باستخدام وسائط إلكترونية بالإضافة إلى نصــوص قانونــية أخــرى تبين ماهية الوسائل التي يتم استخدامها عند جمع الاســتدلالات عن تلك الجرائم و ضبطها و الكيفية البحث عن الأدلة الخاصة بها و الحفاظ عليها و التحقيق في تلك الجرائم تمهيدا للقبض على مرتكبها لينال ما ارتكبت يداه من أفعال ضارة ٠

و يلــزم قبل توافر تلك النصوص القانونية وجود الشرطة الفنية المدربة فنيا و تكنولوجيا على التعامل مع ذلك النوع من الجرائم التكنولوجية الحديثة فيلزم أن تكون أجهزة الشرطة مدربة فنيا بالقدر الكافي الذي يجعلها قادرة على ضبط تلك الجــرائم و الــتعامل مع مرتكبيها و إيجاد الدليل الخاص بها و الحفاظ عليه و ليســت أجهــزة الشــرطة فقط هي التي يجب أن تكون مؤهلة لذلك بل يجب أن يكــون رجال النيابة العامة و رجال القضاء و السادة المحامين يجب أن يكونوا جمــيعا مؤهليــن للتعامل مع ذلك النوع من الجرائم الإلكترونية الحديثة هذا من جهة و من جهة أخرى يلزم توافر الأجهزة الفنية لهم أيضا ليستطيعوا القيام بما

هو منوط بهم من واجبات لإمكانية التعامل معها فالتدريب ألفني فقط لا يأتي بالنتائج المرجوة بل لابد من وجود الأجهزة الفنية التي تعينهم على القيام بمهامهم ٠

هذا ولما كانت الجرائم الإلكترونية التي تقع علي نظم وشبكات الحاسبات والاتصالات في أحيان كثيرة جرائم عابرة للحدود CRIMES TRANS BORDER أي أن مرتكب الجريمة قد يستخدم حاسباً أو جهازاً أو شبكة اتصال في دولة وتقع الجريمة علي حاسب أو نظام أو شبكة اتصال في دولة أخرى فإن الأمر يستلزم وجود اتفاقية دولية تنظم هذه المسائل بين الدول حتى تعدل قوانين العقوبات وقوانين الإجراءات الجنائية في كل منها لتجريم تلك الأفعال - فلا يكون هناك أفعال معاقب عليها في دولة ما و لا يكون معاقب عليها في دولة أخرى و بالتالي تكون الفرصة سانحة أمام مرتكبي تلك الأفعال أن يفلتوا بفعلتهم باللجؤ إلى الدول التي لا تجرم تلك الأفعال - و ذلك كي يتحقق التعاون الدولي بين الدول في تلك الجرائم فلا يفلت الجاني بفعلته علماً أن ذلك التنظيم موجود جزئياً من خلال ما يعرف بمعاهدة بودابست لمكافحة جرائم نظم وشبكات الاتصالات THE BUDAPEST CONVENTION ON CYBER CRIMES والتي لم تنضم مصر إليها حتى الآن.

و عليه ففي مجال عرضنا لتجربة جمهورية مصر العربية في مجال مكافحة جرائم الإنترنت سوف نعرض لعدة نقاط هي : -

- ١ - إصدار قانون حماية الملكية الفكرية
- ٢ - تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت
- ٣ - الانضمام إلى المعاهدات و الاتفاقات الدولية التي تعمل على تجريم جرائم الإنترنت
- ٤ - استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون

- التجارة الإلكترونية و قانون التوقيع الإلكتروني
- ٥ – إنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن تلك الجرائم
- ٦ – تحقيق الأمن المعلوماتي للكيانات الاقتصادية

١ – إصدار قانون حماية الملكية الفكرية

كانت جمهورية مصر العربية من أولى الدول العربية التي انضمت إلى كافة المعاهدات و الاتفاقات الدولية التي كانت تعمل في مجال حماية حقوق الملكية الفكرية من القرصنة و تأسيسا على هذا الاهتمام فقط انضمت مصر إلى معاهدة برن و تريبس و معاهدات الويبو و كان من نتيجة هذا الاهتمام أن أصدرت مصر قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ و الذي يوفر الحماية لمصنفات الحاسب الآلي لمدة خمسون عاما من تاريخ وفاة المؤلف أو من تاريخ النشر .

أما عن الحقوق التي يتمتع بها المؤلف طبقا لهذا القانون فقد نص القانون على تمتع المؤلف وحده بالحق في الترخيص أو عدم الترخيص لأي جهة بأستغلال مصنفه سواء بالنسخ أو البيع أو التأجير أو الإعارة أو إتاحته عبر أجهزة الحاسب الآلي و شبكة الإنترنت و غيرها من شبكات المعلومات و وسائل الاستغلال .

و يحظر القانون الآتي : -

- أي نسخ كلي أو جزئي للبرامج أو الاقتباس منها إلا بعد الحصول ترخيص كتابي مسبق من المؤلف أو من الممثل القانوني له
- إزالة أو تعطيل أو التغييب لأي حماية تقنية يستخدمها المؤلف كالتشفير

- أو غيره
- تقليد أو بيع أو عرض للتداول أو للإيجار في مصر مصنفا منشورا في الخارج أو تصديره ٠
- النشـــر عـــبر أجهـــزة الحاســـب الآلي أو شبكات الإنترنت أو شبكات المعلومـــات أو شبكات الاتصالات أو غيرها من شبكات و الوسائل دون إذن كتابي مسبق من المؤلف
- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف

العقوبات التي تقررت بموجب قانون حماية الملكية الفكرية : -

الجزاءات الجنائية : -

- يعاقب المعتدى بالحبس من شهر حتى ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف جنيه لكل برنامج أو بإحدى هاتين العقوبتين
- بإغلاق المنشأة التي استغلها المقلدون أو شركاؤهم كما يجوز للمحكمة أن تقضي مدة لا تزيد على ستة أشهر
- وفى حال معاودة المخالفة يصبح الحبس وجوبيا بحد ادني ثلاث شهور مـــع غـــرامة مالية قد تصل إلى ٥٠ ألف جنية ويصبح غلق المنشأة وجوبيا
- وتـــتم في كل الأحوال مصادرة النسخ المقلدة والأدوات المستخدمة في الاعتداء
- ينشـــر ملخـــص الحكم الصادر بالإدانة في جريدة يومية واحدة أو أكثر على نفقة المحكوم عليه

الجزاءات المدنية : -

- يســـتحق المؤلـــف أو من يخلفه في حال الاعتداء على حق أو أكثر من حقوقـــه و الحصول على تعويضات مدنية عما لحقه من أضرار أدبية

- ومالية قد تصل إلى ملايين الجنيهات ٠
- يلـــزم القـــانون كـــل المحـــال التي تطرح للتداول بالبيع أو بالإيجار أو بالإعـــارة أو بالترخـــيص بالاستخدام مصنفات الحاسب الآلي أو قواعد البـــيانات بالحصـــول علـــي ترخـــيص بذلـــك مـــن وزارة الاتصالات والمعلومات ويعاقب علي مخالفة هذه المادة بغرامة لا تقل عن خمسة آلاف ولا تزيد عن عشرين ألف جنيه مصري ٠
- يلزم القانون ناشرو وطابعو ومنتجو مصنفات الحاسب الآلي أو قواعد البيانات بإيداع نسخة من المصنف أو اكثر بما لا يجاوز العشرة ويعاقب علي مخالفة هذه المادة بغرامة لا تقل عن ألف جنية ولا تزيد عن ثلاثة عن كل مصنف

٢ – تحديـــث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت

MODERNISATION THE REIGNING LAWS TO A NEW LAWS CRIMINALISING THE INTERNET CRIMES

حتى الآن لم يتم استحداث أي قوانين جديدة في جمهورية مصر العربية تجارى التطور الحادث في نوعية الجرائم و طرق ارتكابها – فحتى الآن يتم إدراج تلك الجـــرائم الإلكترونـــية التـــي ترتكب عبر شبكة الإنترنت تحت نصوص القوانين القديمـــة و يـــتم تطبيق العقوبات القديمة عليها رغم أن تلك الجرائم تحتاج إلى غلظـــة العقوبة حتى تكون المحاولة جادة في الحد من ارتكاب تلك اللجرائم – و كان يجب أن تكون تلك القوانين قد تم سنها منذ أن انتشرت خدمة الإنترنت في

مصر على نطاق واسع لان انتشارها على نطاق واسع سيؤدى بالطبع إلى زيادة الاحتمال باستخدامها استخداما سيئا في ارتكاب الجرائم الجديدة على المجتمع و بالتالي كان يجب أن تكون تلك القوانين جاهزة للتطبيق لا أن يتم التفكير في سنها بعد أن زاد ارتكاب تلك الجرائم بكافة أنواعها ،

إلا انه في نفس الوقت لابد من الإشارة إلى أن ارتكاب تلك الجرائم لازال في مراحله الأولى رغم الانتشار السريع للإنترنت في مصر نظرا لطبيعة المصريين و ما يحكمهم من عادات و تقاليد تحد كثيرا من أي نزعات إجرامية قد تكون موجودة في أي فئة من فئات البشر فالطبيعة السمحة و تقربهم من الدين و التزامهم بأوامره و نواهيه تعمل على الحد من نسبة ارتكاب الجرائم عنها في أي بلد من بلاد العالم مهما يتاح لهم من وسائل ارتكابها ،

و عملية تحديث القوانين لا تتم في جمهورية مصر العربية بالسرعة المطلوبة لتجارة التطور الحادث في التكنولوجيا و وسائل الاتصال و عمليات التجارة الإلكترونية و ما إلى ذلك من تطور حاصل في كافة المعاملات التي تتم باستخدام احدث ما وصل إليه العالم من التكنولوجيا و سوف نعرض فيما يلي بعض من أهم القوانين التي لا يجب التأخر في عمليات التحديث الخاصة بها حتى لا نبتعد عن عمليات التطور التي تحدث يوميا و لكي لا تزداد الهوة التكنولوجية التي تعمل على زيادة الفارق فيما بين الدول المتقدمة و الدول النامية ،

و من أهم القوانين التي تحتاج إلى تحديث : -

١ - تلك القوانين التي تتعلق بمأموريات الشهر العقاري و التوثيق و اللوائح الخاصة بها و أهمية تحديث تلك القوانين و اللوائح لكي تتواءم مع العاملات الجديدة - المعاملات الإلكترونية - و من نواحي التحديث التي يمكن طرحها انه يمكن اعتماد مصلحة الشهر العقاري و التوثيق لتصبح هي الجهة المؤتمنة علي

حفظ الوثائق الإلكترونية واعتمادها - الطرف الثالث المحايد المودع لديه الوثيقة - أو يمكن إيجاد جهات حكومية أخري تتسم بالنزاهة والحيدة كهيئة البريد للقيام بتلك المهمة .

٢ - تحديث القوانين المنظمة لهيئة سوق المال و كذلك القوانين المنظمة للبورصات و اللوائح الخاصة بها و ذلك لأمر هام حيث انه من الضروري تحديث التعاملات التي تتم على الأسهم و السندات ليكون في الإمكان التعامل على الأسهم و السندات المصرية بالأساليب الإلكترونية الحديثة و بالتالي يمكن جذب رؤوس الأموال الأجنبية للاستثمار في مصر حيث انه بدون تحديث تلك القوانين و تقنين الأساليب الحديثة الإلكترونية ستتعاظم الفوارق التي تفرق بيننا و بين الدول المتقدمة تكنولوجيا .

٣ - نوع آخر من القوانين لابد من التعامل معه بمزيد من الأهمية لأنه يؤثر كثيرا مع رؤوس الأموال الأجنبية التي لابد من جذب الكم الأكبر منها إلى مصر فالتشريعات و اللوائح الضريبية لابد من تحديثها ليكون في إمكانها العمل في عصر يتم التعامل التجاري فيه إلكترونيا دون أي يرى أي من أطرافه الطرف الآخر و عليه فلابد من تحديث تلك التشريعات التي تحكم المجال الضريبي في مصر ليجارى التطور الجاري في المجال التجاري الدولي و إلا فلن تتمكن الدولة من تحصيل ما تستحقه من حقوقها الضريبية على ما يتم من معاملات تجارية تتم إلكترونيا دون أن تكون الدولة قادرة على متابعتها و بالتالي تقف القوانين عاجزة عن أن تحصل حقوق الدولة .

٤ - أما عن التشريعات الجمركية فالحال مع التشريعات الضريبية هو نفسه الحال مع التشريعات الجمركية إذ انه لابد من تحديث تلك التشريعات الجمركية أيضا و بالتوازي مع التحديث الذي يجب إتمامه مع التشريعات الضريبية بل و مع كافة التشريعات الأخرى التي يتم تحديثها فالتأخير في تحديث تلك التشريعات

يؤثـــر على التعاملات التجارية التي تتم بين مصر و العالم الخارجي الذي اصبح التعامل بينه و بين بعضه الآخر إلكترونيا صرفا دون أن يكون فيه أي دور لتلك التشريعات القديمة التي عفي عليها الزمن ٠

٥ – لمـــا كـــان لا يمكن الفصل بين التعاملات الداخلية التجارية التي تتم داخل البلد الواحد و بين التعاملات التجارية التي تتم بين الدول كان من اللازم تحديث تلك القوانين الداخلية التي قد يرى البعض انه لا فائدة كبيرة من تحديثها و هو رأى خاطـــئ لان الـــتعاملات الـــتجارية الداخلـــية هي امتداد طبيعي للمعاملات التجارية الخارجية و عليه فتحديث القوانين التي تستخدم في التعاملات التجارية في داخل مصر هو أمر ذو أهمية قصوى و من تلك القوانين قانون المناقصات و المزايدات و التوريدات و أهمية ذلك التحديث ليكون هناك توافقا و تلائما بين تلك القوانين و طبيعة التجارة الإلكترونية

٦ – أما التشريعات الخاصة بحماية المستهلك في مجال التجارة الإلكترونية فهي مـــن أهـــم التشريعات التي يجب أن تكون لها الأولوية في التحديث لان تحديث القوانيـــن فـــي كافـــة المجالات هدفه الأول هو تقوية الاقتصاد الوطني و هدف تقويـــة الاقتصاد الوطني هو تحسين الحالة الاقتصادية للمستهلك لأنه الأساس فـــي كل ذلك و بالتالي فأن القوانين التي تستهدف حماية المستهلك هي الأولي فـــي أن تنال الأولوية في التحديث لا أن يتم إهدارها و إهمالها و إغفال دورها في حماية المستهلك ٠

٧ – تعديـــل قانونـــي العقوبات والإجراءات الجنائية ليكون النص فيهما صريحا علـــى تجريم جرائم الإنترنت و الحاسبات الآلية بدلا من إدراج تلك الجرائم تحت النصـــوص القانونية القديمة و تحت مسمى الجرائم التقليدية القديمة لعدم وجود نصوص قانونية جديدة تنص صراحة و بوضوح على تجريمها ٠

فيكـــون هنـــاك نصـــوص تنص صراحة على تجريم التشهير عبر الإنترنت و

نصـــوص أخـــرى تجرم الاحتيال عبر الإنترنت و أيضا أفعال الاعتداء علي نظم وشـــبكات الحواســـب المعلوماتـــية والاتصـــالات أو اســـتخدام تلـــك الوســـائل والتكنولوجـــيا الحديـــثة فـــي الاعتداء علي الأشخاص والأموال وكذلك الدولة و الأفـــراد و الهيـــئات أو الشـــركات و النصـــب والغـــش والاحتيال والقرصنة المعلوماتـــية و هكـــذا تكون هناك نصوص تنص صراحة على تجريم أي جرائم يمكـــن أن ترتكـــب عـــبر الإنترنـــت إلا انه يجب أن تراعى أيضا أن تكون تلك النصوص قد صيغت على أساس أن تستوعب أي تطوير قد يحدث في المستقبل – على الأقل القريب – في طرق و وسائل ارتكاب مثل تلك الجرائم ٠

كمـــا انـــه من المستحسن على النص صراحة على الأساليب التي يجب أن تتبع عـــند جمع الاستدلالات و التفتيش و التحقيق و ضبط وحفظ الأدلة الجنائية في الجـــرائم المعلوماتـــية تحديـــداً للمسئولية الجنائية وحماية للتجارة الإلكترونية والمعاملات الإلكترونية

هـــذا مـــن جهة و من جهة فلابد من من تنظيم الدورات التعليمية الكافية لرجال البحـــث القضـــائي و أعضاء النيابة العامة و أعضاء الهيئات القضائية و كذلك الســـادة المحـــامون لتدريـــبهم علـــى الوســـائل و الأدوات الإلكترونية لفهما و اســـتيعابها ليتمكنوا من القيام بما هو منوط بهم في أعمالهم على الوجه الأكمل دون أي تقصير ٠

٣ – الانضـــمام إلى المعاهدات و الدولية التي تعمل على مكافحة جرائم الإنترنت

كانـــت حكومـــة جمهورية مصر العربية على قناعة تامة و منذ البداية على أن الانضمـــام إلى المعاهدات و الاتفاقات الدوليـــة هـــو من أهم الوسائل التي يجب

الأخــذ بها و اتباعها في مجال مكافحة جرائم الإنترنت و عليه فلم تتوان مصر فــي الانضمام إلى كافة المعاهدات الدولية التي تم عقدها في هذا المجال و ذلك إيمانــا مــنها بأن الانضمام إلى الأسرة الدولية هو من أهم الوسائل التي يجب اتباعها في مجال مكافحة جرائم الإنترنت ٠

و يجب أن نربط هنا بين التعاون الدولي في مكافحة جرائم المعلومات و ما تقوم بــه مصــر مــن خطوات هامة في هذا المجال فالتعاون الدولي الهام يتمثل في أوضح و أهم صوره في المعاهدات و الاتفاقات الدولية التي يتم عقدها سواء في مجــال مكافحــة جــرائم الإنترنت و أيضا في مجال حماية الملكية الفكرية و قد انضمت مصر إلى الاتفاقات الدولية الخاصة بحماية حق الملكية الفكرية كما أنها أصــدرت قــانون حمايــة الملكية الفكرية الخاص بها و الصادر برقم ٨٢ لسنة ٢٠٠٢ و قد كانت المعاهدات الدولية كمعاهدة برن و معاهدة تريبس و معاهدات الويــبو هما الأساس الذي تم بناء عليهم سن هذا التشريع الذي تنضم به مصر إلى الأسرة الدولية في مجال حماية الملكية الفكرية ٠

و من جهة أخرى فقد قامت مصر أيضا بمسايرة الأسرة الدولية فيما تبنته هيئة الأمــم المــتحدة مــن إصــدار قوانيــن خاصة بالتجارة الإلكترونية و التوقيع الإلكتروني و قد تم ذلك أيضا إيمانا من مصر بأن الانضمام إلى المجتمع الدولي فيه الخير و الفائدة إلى جمهورية مصر العربية ٠

و مــثال ذلــك أيضا انضمام مصر إلى كافة الاتفاقات العربية التي اقرها مجلس وزراء الداخلــية العــرب و كذلك مجلس وزراء الداخلية و العدل العرب و هي اتفاقــات عربــية تهــدف إلى التعاون فيما بين الدول العربية في مجال مكافحة الجــريمــة المــنظمة و الاتجــار فــي المخدرات و المؤثرات العقلية و مكافحة الإرهاب ٠

٤ - استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون التجارة الإلكترونية و قانون التوقيع الإلكتروني

تلعب التجارة الإلكترونية ELECTRONIC COMMERCE بصفة خاصة و التطور الهائل في تقنيات الاتصال و المعلومات بصفة عامة دورا اقل ما يوصف بأنه هائل جدا في تطور الاقتصاد العالمي بصفة عامة و الاقتصاد الوطني بصفة خاصة فلا يمكن إنكار أن التجارة الإلكترونية عملت و بشكل كبير جدا على سرعة انتقال المعاملات و رؤوس الأموال و ألغت ما كان يعوقها قديما من الحواجز الجغرافية التي كانت تحد كثيرا من حركتها و كذلك قلة المعلومات التي كانت تعتبر في الماضي الحاجز الأكبر في عدم اجتياز اقتصاد الدول النامية في النفاذ إلى العالمية و الحصول على نصيبه الطبيعي من حجم التجارة الدولية .

إلا انه و من جهة أخرى فأن التفاوت التكنولوجي فيما بين الدول المتقدمة و الدول النامية قد يؤدى إلى عدم استفادة اقتصاد الدول النامية من ذلك التقدم التكنولوجي الهائل الذي يعيشه العالم حاليا و المسمى التجارة الإلكترونية و عليه فصحيح أن الحواجز التي كانت تعوق الدول النامية قد زالت إلا انه قد وجد مكانها حاجز آخر ألا وهو التقدم التكنولوجي الذي يعتبر اسهل ولو جزئيا في إمكانية تجاوزه و العمل على التفوق فيه مع أهمية ملاحظة أن عدم قدرة الدول النامية على تجاوز مثل هذا الحاجز فسوف تزيد الهوة فيما بينها و بين الدول المتقدمة و أن يفيد عندئذ أي مجهود قد يبذل للعمل على تقليله .

هذا و يعد الإنترنت هو القوة الدافعة في انتشار التجارة الإلكترونية ELECTRONIC COMMERCE و بعد ما وفرته شبكة الإنترنت من سرعة قصوى في تناقل البيانات و الأموال و الوثائق في اقل من ثواني

قليلة مهما كانت المسافة التي تفصل بين الأطراف فشبكة الإنترنت تعد هي الوسيلة الوحيدة في إبرام الصفقات في الكثير جدا من الصفقات في الوقت الحالي ٠

و رغم أن العديد من الدول النامية لم تستفيد حتى الآن من تلك التكنولوجيا المتطورة نظرا لعدم وجود البنية التحتية لخدمات الاتصالات الهاتفية إلا أن جمهورية مصر العربية ليست كذلك ٠

فجمهورية مصر العربية لديها بنية تحتية متكاملة جدا في مجال الاتصالات الهاتفية و هو ما جعلها تستفيد أقصى استفادة و جعل انتشار شبكة الإنترنت INTERNET يتضاعف سنويا بل انه قد يكون يتضاعف اكثر من مرة في العام الواحد ٠

و يتمثل ذلك في زيادة الخدمات الهاتفية في مصر خلال السنتين الأخيرتين بنسبة كبيرة لتصل عدد الخطوط الثابتة إلى ٨,٦ ملايين خط تليفوني بزيادة شهرية قدرها ٨٠٠٠٠ خط جديد كما زادت نسبة انتشار التليفون المحمول في مصر لتصل إلى ٥ % سنويا أي ٥,٣ ملايين مشترك وهذا يرجع إلى اهتمام الحكومة المصرية بتطوير البنية الأساسية للمعلومات والاتصالات الهاتفية فمنذ عام (١٩٨٥) اتخذ قرار لإنشاء البنية الأساسية للمعلومات الوطنية لتصبح الأساس لتطوير جميع القطاعات والصناعات بمشاركة القطاع العام مع القطاع الخاص، وخلال الفترة من ٨٥ - ٩٥ تم إنشاء أكثر من ٦٠٠ مركز لدعم واتخاذ القرار في ٢٦ محافظة بهدف تطوير التجارة والحياة الاقتصادية والاجتماعية.

كما أن مصر تنظر إلى التجارة الإلكترونية ELECTRONIC COMMERCE كداعم أساسي للتجارة وخطط التقدم الاجتماعي والاقتصادي حيث تقدم التجارة الإلكترونية فرصا لزيادة حجم التجارة وتنشيط

الاستثمار وتسهيل الصفقات التجارية بالإضافة إلى أنها تتيح أسواقاً أكبر وأكثر تنوعا وطرقاً تسويقية جديدة ويتوقع أن يصل حجم التجارة الإلكترونية إلى أكثر مـن تريلـيون دولار أميركي وهذه الزيادة في حجم التجارة تحمل في طبائعها مـزايا كامـنة للاقتصاد المصري إذا استطاع استخدامها جيدا وخاصة بالنسبة للمشـروعات الصغيرة والمتوسطة والتي قبل استخدام التجارة الإلكترونية كانت تفتقر السبل لترويج منتجاتها بالخارج.

كمـا انه من المعروف أن التجارة الإلكترونية لا تقتصر فقط على التجارة و إنما تمـتد لتشـمل قطاعـا كبيرا من الأعمال كالخدمات المالية كالتامين و البنوك و الـتجارة و السـياحة و الترفـيه و الدعاية و التسويق و المعلومات والتعليم و التدريب و الإعلام كالكتب الإلكترونية ٠

و لـتكون الـتجارة الإلكترونية موجودة في بيئة صحيحة و ليتم الاستفادة منها أقصى استفادة فقد قامت مصر باتخاذ عدد من الخطوات نوجزها فيما يلي : -

- و قد تم إصدار قانون يقنن التجارة الإلكترونية في مصر
- و كذلك أصدرت قانون آخر لتقنين مسألة التوقيع الإلكتروني
- تطويـر البنية الأساسية للمعلومات بإنشاء العديد من مراكز المعلومات على مستوى الجمهورية
- تنفـيذ العديـد مـن المشـروعات التـي تعتمد و بشكل أساسي على الصـناعات ذات التكنولوجـيا العالية لنقل تلك التكنولوجيا إلى داخل مصر
- زيـادة الوعي من جميع الجهات المعنية بالاستفادة من تلك التكنولوجيا المـتقدمة و العمل على فتح منافذ للصناعات المصرية عبر تلك البوابة الإلكترونية التي تختصر الكثير من الوقت و المسافات ٠

ورغـم أن مصـر قد خطت الكثير من الخطوات في مجال التجارة الإلكترونية و تنشـيطها و الاسـتفادة منها إلا أن الأمن هو من اكبر المشاكل التي تعرقل مثل هذه الخطوات .

فالحفـاظ علـى السرية والخصوصية هو من أهم المشكلات التي تواجه التجارة الإلكترونية ليس في مصر فقط بل في العالم اجمع .

فلابـد من التأكيد على السرية و الخصوصية فيما يتعلق بالبيانات و المعلومات التـي يـتم تداولها على شبكة الإنترنت في مجال التجارة الإلكترونية و لابد من النص قانونا على الحفاظ على تلك السرية إذا أردنا على الاستفادة .

ورغـم أنـنا نطالب بالنص قانونا على الحفاظ على السرية إلا أن تلك السرية يمكن أن تنتهك عبر الشبكة دون إمكانية التحقق من الهوية .

فعـدم القـدرة على التأكد من هوية المستخدم والتحقق من المعاملات من أكبر المشـاكل التـي تواجه التجارة الإلكترونية ويعتبر النقص في تحديد الهوية من الأسباب الرئيسية لتسهيل الاحتيال والخداع ويمكن أن يؤدي إلى جرائم عديدة لا يمكـن ارتكابها في الأسواق التقليدية بنفس الطريقة فالاحتيال عن طريق كروت الائـتمان يمكـن أن يظهـر عندما يطلب التجار دليلا حقيقيا والذي لا يمكن أن يمتلكه إلا المالك الحقيقي .

كمـا أن الـنظام الورقـي البنكي الحالي يعوق التجارة الإلكترونية ولا يوجد ما يعوق البنوك بشكل قانوني من استخدام الإنترنت ولكن بسبب المخاوف المتعلقة بالأمـن فـإنهم لا يشعرون بالراحة من تبادل الصفقات و البيانات عبر الإنترنت لذلـك فـإن البـنوك لا تقبل الدفع عبر الإنترنت ولا تبادل الصفقات حتى لو لم يكونـوا ممنوعيـن بشـكل رسمي من ذلك ويرجع الرفض السائد لدى البنوك المصـرية فـي تسـهيل الائتمان عبر الإنترنت والتبادل التجاري لنقص ضمان السرية و الأمن بخصوص إجراء تلك العمليات كما أن أعمال البنوك المحدودة

عــبر الإنترنــت كانــت مقصودة ولكن إضافة إلى ذلك فقد تم التبليغ عن بعض عمليات الاحتيال التي تمت و لم يتم تحديد هوية مرتكبيها •

٥ – إنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن تلك الجرائم

أنشأت وزارة الداخلية في جمهورية مصر العربية إدارة جديدة تماما في تكوينها و نوعــية عملها جديدة في تكوينها لأنها تتكون من ضباط على أعلى درجة من التخصــص و الحرفــية في تكنولوجيا الحاسبات و شبكة الإنترنت و جديدة في نوعــية عملهــا على أساس أن عملها ليس ضبط المجرمين التقليدين الذين لا زالــوا يرتكبون جرائمهم بالطرق التقليدية القديمة المحفوظة لدي كافة العاملين بــوزارة الداخلية المصرية و إنما لملاحقة مجرمين على درجة تقنية عالية في مجــال الحاســبات و شــبكة الإنترنت و يرتكبون جرائمهم بطرق متطورة على المجــتمع مســتخدمين فيها تكنولوجيا الحاسبات و شبكة الإنترنت و يكون من الصــعب أن لــم يكــن من المستحيل أن تتم ملاحقتهم إلا باستخدام وسائل اكثر تطــورا و بواســطة ضباط على أعلى درجة من التدريب و التخصص على تلك التكنولوجيا •

و قــد تم إنشاء تلك الإدارة الجديدة بعد أن زاد عدد مستخدمي شبكة الإنترنت خاصة بعد أن اصبح الدخول على الشبكة يتم بسهولة كبيرة جدا و لا يحتاج إلى أي تعقــيدات كما كان في أول الأمر عندما كانت في بدأ دخولها إلى مصر إذ أن الدخول علي شبكة الإنترنت الآن لا يحتاج إلا إلى خط تليفون و جهاز كومبيوتر بالطبع •

و بالطبع و مع زيادة عدد مستخدمي الإنترنت زاد بالتالي من يقومون باستخدام تلـك التكنولوجيا استخداما سيئا و يستغلونها في ارتكاب جرائمهم معتقدين انهم بعـيدون جدا عن أيدي القانون و بعيدين عن أن ينالوا عقابهم على ما ارتكبت أيديهـم فعـدد الجـرائم التـي ترتكـب باستخدام تلك الشبكة و عليه كان من الضـروري إنشاء تلك الإدارة ليكون في الإمكان الحد من تلك الجرائم و محاولة منعها نهائيا أن أمكن

و قـد تلاحـظ أن معظـم تلـك الجـرائم التي ترتكب على الشبكة أو باستخدام الحاسبات يكون تكييفها القانوني متوافق في معظم الأحيان مع التكييف القانوني التقلـيدي المنطـبق على نفس الجرائم التي ترتكب بالطرق التقليدية مع وجود فـراق واحـد فقـط هو أداة الجريمة أي استخدام الحاسبات أو شبكة الإنترنت INTERNET في ارتكاب الجريمة أي استخدام التقدم التقني MODERN TECHNIQUES فـي ارتكاب الجرائم بدلا من الطرق التقليدية التي كانت تلـك الجـرائم ترتكب بها دائما في الماضي و هو بالتالي ما يضعها تحت طائلة القـانون LAW دون الحاجـة إلـى وجود نصوص قانونية جديدة تجرم تلك الجرائم CRIMES ٠

و وجد أن معظم ما تم ضبطه من جرائم هي في الغالب جرائم ابتزاز و تشهير و نصـب و احتـيال و سرقة و دعارة و إنما هي تتم بطرق تكنولوجية حديثة لم يكـن فـي الإمكان كشفها و ملاحقة مرتكبيها أو ضبطهم إلا بوجود تلك الإدارة التي تم إنشائها حديثا ٠

و نحـن نـرى أن مـن أهـم ما قامت به تلك الإدارة هو ملاحقة القائمين على المواقـع الإباحية التي يتم بثها من داخل البلاد فتلك المواقع بما تبثه من سموم تعمـل علـى إثـارة الغرائز فتؤدى إلى ازدياد الجرائم الجنسية و إغلاق تلك المواقع و ملاحقة القائمين عليها يعمل على الحد من الجرائم الجنسية التي تقع

بسـبب زيـارة تلك المواقع و ما تقوم به من إثارة الغرائز لدى الشباب بصفة خاصة و الرجال بصفة عامة

و نحـن نـرى أيضـا أن وجود نصوص قانونية يتم تطبيقها على تلك الجرائم الحديـثة MODERN CRIMES لا يغنى عن الحاجة إلى وضع نصوص قانونـية جديدة و متطورة تغطى تلك الجرائم الجديدة و ما قد يستجد عليها من جرائم فالتطور التقني MODERN TECHNIQUES الذي نعيشه حاليا و الذكاء و درجة التقنيـة العالية التي يكون عليها هؤلاء المجرمين تنبأ بأنه و فـي المسـتقبل القريب سنواجـه العديد من الجرائم شديدة التعقيد و التطور و التـي لا تجـد لهـا نصـا قانونيا تقع تحت طائلته من تلك النصوص القانونية التقلـيدية القديمـة التي تضع الجرائم التي ترتكب حاليا في نطاقها فنحـن في حاجـة إلى نصوص قانونية جديدة بحيث تجرم تلك الجرائم التكنولوجية الجديدة و مـا قـد يسـتجد عليها من جرائم و من تطور في أدوات ارتكاب مثل تلـك الجرائم حتى لا يأتي الوقت الذي تقف فيه يد القانون عاجزة عن أن تقتص حق المجـتمع مـن تلـك الفئة المنحرفة التي تستغل التكنولوجيا الحديثة و التطور التقنـي MODERN TECHNIQUES فـي ارتكـاب الجرائم بدلا من استغلالها في ما يفيد المجتمع و الاقتصاد الوطني •

علـى انـه يمكن أن تتم الاستعانة عند وضع مثل هذا القانون الجديد بالقوانين التـي وضـعتها الدول المتقدمة في هذا المجال للعمل على توحيد القوانين التي تعـالج تلك الجرائم في جميع الدول و ذلك في محاولة للحد من مثل تلك الجرائم ليس على المستوى المحلى فقط و إنما على المستوى العالمي أيضا •

وفـي هذا المجال يمكن أن يكون للأمم المتحدة الدور الريادي في ذلك فعليها أن تتصـدى لمـثل هـذا الموضـوع بـأن تعمل على وضع قانون نموذجي موحد UNIFIED MODEL LAW بحيـث يكون على الدول عند وضع قانونها

المحلى أن تقتبس منه ما هو مناسب لمجتمعها و تقاليدها و بالتالي يكون هناك الحد الأدنى على الأقل في التماثل و التناسق بين القوانين التي تعالج هذا الموضوع على المستوى العالمي وهو ما يعمل على الحد من ارتكاب مثل تلك الجرائم و أيضا لابد من وجود تناسق في القوانين لمواجهة الجرائم التكنولوجية الحديثة التي تكون في الأغلب الأعم من الحالات هي جرائم عابرة للحدود CRIMES TRANS BOEDER و لمواجهتها لا بد من وجود مواجهة لها من كافة القوانين الموضوعة على المستوى المحلى و الدولي ٠

٦ - تحقيق الأمن المعلوماتي للكيانات الاقتصادية

تعد الكيانات الاقتصادية متمثلة في الشركات و البنوك و ما شابه ذلك من الركائز التي يرتكز عليها أي اقتصاد وطني و عليه فحماية الأمن الإلكتروني لتلك الكيانات هو من الأولويات التي يجب تحقيقها في الاعتبار على وجه السرعة و دون أي إبطاء قد يتسبب في اختراق تلك المنشآت و ما قد يتسبب فيه ذلك من خسائر مادية و معنوية هائلة لتلك المنشآت و مستوى سمعتها العالمية من الثقة و الآمان ٠

و عليه فقد تمت دراسة المحاولات التي يمكن بذلها لاختراق تلك الكيانات الاقتصادية و الحلول التي تم وضعها لمنع حدوثها

١ - محاولات الاختراق

١ - أن ضغط المعلومات علي وسيط معلوماتي في حيز دقيق هو بالقطع أمر مفيد للمنشأة ولكنه قد يصبح عنصر خطر فالأسرار التجارية المالية والصناعية

يــتم تخزيــنها فــي وســائط معلوماتــية مضغوطة دقيقة الحكم يسهل سرقتها وإخــراجها مــن المنشــأة فــي حيز لا يزيد علي علبة السجائر كما يمكن نقل المعلومــات المالية والتجارية والصناعية المخزنة إلكترونياً في لحظات معدودة غير شبكات الحواسب والاتصالات.

٢ - إن اللامركــزية فــي حفــظ واسترجاع المعلومات الحساسة إلكترونياً لها مخاطــرها ففــي بعــض المنشآت يكون للعاملين حرية وقدرة الدخول إلي نظم المعلومات والاتصالات الخاصة بشبكة حواسب المنشأة ويمكن لهم في حالة عدم وجــود نظــام أمن معلومات وأمن اتصالات أن يغترفوا مثل هذه المعلومات وأن يستخدموها بشكل غير أمين أو غير مشروع يضر بالمنشأة.

٣ - إن اســتخدام وســائل الاتصــالات غــير المشــفرة لنقل رسائل البيانات الإلكترونــية وغــيرها مــن المعلومات يعرض المنشأة التجارية لمخاطر أنشطة إجرامية من منشآت منافسة .

٤ - إن سهولة نقل المعلومات باستخدام البرمجيات ووسائل الاتصالات الحديثة دون تأميــن أدوات المعلومــات والاتصــالات يعــرض أسرار المنشأة التجارية لمخاطر جسيمة.

٥ - أن تحــرك وتنقل وسفر المسئولين عن المنشأة التجارية بأجهزة حاسبات نقالــة غــير مؤمــنة تحــتوي علي معلومات دقيقة وحساسة خاصة بالمنشآت وأنشــطتها التجارية والمالية يعرض تلك البيانات والمعلومات لمخاطر في حالة سرقة تلك الأجهزة أو الدخول إليها من شخص غير مرخص له .

٦ - أن عــدم تأميــن نظم الاتصالات والحاسبات والمعلومات يعرض ممتلكات الشــركــة وبــياناتها للتخريب والتدمير خاصــة في حالة عدم وجود نظم حفظ بديلــــة .

٧ - إن استخدام المقاولين من خــارج المنــشأة SURCING OUT في

عمليات إنشاء أو حفظ أو إدارة نظم الحاسبات والمعلومات والاتصالات الخاصة بالمنشـأة قـد يعرض المنشأة لمخاطر جسيمة وقد يعرض أسرارها لمخاطر لا يعـرف مداها سواء عن طريق الموظفين التابعين لذلك المقاول أو المقاول ذاته سواء كان موجوداً في الموقع - ركز المنشأة - أو يتعامل ويتصل بالنظام من خارج المنشأة و عليه لابد من التأكد من السمعة الممتازة لهؤلاء المقاولين قبل إسـناد تلك العمليات لهم مع مراقبة تنفيذ الأعمال بواسطة استشاري متخصص محايد وحسن السمعة .

٨ - إن الإدارة التـي ليست على قدر من الكفاءة لتدير نظم وشبكات المعلومات والاتصالات داخل المنشأة قد تعرض بيانات المنشأة وممتلكاتها لمخاطر جسيمة ومن ذلك الاختراق من قبل أشخاص أو جهات علي مستوي احتراف عال أو من موظفين من ذات المنشأة .

٩ - أن ضـعف الوعـي بأمن المعلومات وآمن الاتصالات في المنشأة قد يكون مصدر خطرٍ ففي المنشأة الكبرى قد يوجد مسئولين أكفاء عن أمن المعلومات و أمن الاتصالات ولكن في الشركات متوسطة الحجم أو المنشأة الفردية قلما يوجد متخصص في أمن المعلومات و أمن الاتصالات.

إضـافة إلـي الاخـتراق المادي الملموس لنظم ومنشآت الحاسبات والاتصالات المتمثل مثلاً في سرقة وسائط إلكترونية مشحونة بالبيانات أو تكسير المعدات أو إتلافها الخ فإن من الوسائل الفنية للاعتداء علي نظم المعلومات والاتصالات ما يلي :-

١ - اخـتراق شـبكات الاتصـالات بوسائل مادية بالدخول إلي الخط التليفوني الواصـل للمنشأة عبر وصلة سلكية مادية وذلك للحصول علي معلومات صوتية أو بيانات منقولة .

٢ - التصنت علي المكالمات التليفونية باستخدام وسائل فنية مثل DIALER NUMBER RECORDER (DNR)

٣ - استخدام وسائل مثل جهاز ماسح الموجات SCANNER للتنصت علي الاتصالات الخاصة بالمحمول وخلافه.

٤ - وضع أجهزة تنصت في أجهزة الحاسبات أو الاتصالات الخاصة بالمنشأة أو في غرف اجتماعاتها.

٥ - عدم الكشف علي البرمجيات التي يتم إعدادها للمنشأة من قبل مهندسي برمجيات للتأكد من وجود أو عدم وجود أوامر نائمة أو مدفونة لإساءة استخدام البرمجيات في الحال والاستقبال عند تشغيل تلك البرمجيات.

٦ - وجود ثقب HOLE أو ثقوب في نظم الحاسبات أو البرمجيات قد يؤدي إلي إمكانية اختراق نظم المعلومات والاتصالات لاغتراف المعلومات أو تغير البيانات والعبث بها أو تدمير نظم المعلومات والشبكات.

٢ - وسائل الآمان التي يجب أن تتبع

يشمل أمن المعلومات والاتصالات استخدام وسائل تقليدية لتحقيق الأمن وكذلك وسائل حديثة غير تقليدية.

أ - الأساليب التقليدية للأمن بالأجهزة والمنشآت :-

يشمل ذلك نظم الحراسة والأسوار والبوابات المؤمنة ووسائل الإنذار ضد الاختراق أو الحريق وتكون درجة الأمن التقليدي متناسبة مع أهمية وحساسية وموقع منشآت وأجهزة الاتصالات أو المعلومات أو الحاسبات المطلوب حمايتها ويقوم الأمن التقليدي علي عناصر فنية وإدارية و هندسية بوجود إدارات الأمن في المنشآت واستخدام الوسائل والأدوات الفنية التقليدية في الحماية والتأمين

إضـــافة إلي التصميم الهندسي الآمن لتلك المنشآت وصفوة القول في هذا المقام هو ما قرره عالم حديث من أن الأمن التقليدي يتمثل في الحراسة و التحصين و التشريع و التدريع و القفل والفتح .

ب - الأساليب والوسائل غير التقليدية

أن تحقـيق أمـن المعلومـات و أمن الاتصالات في المنشأة يتمثل في ضرورة وجـود نظام كفء لإدارة المعلومات MANAGEMENT SYSTEM OF INFORMATION وأمن المعلومات والاتصالات ويشمل ذلك : -

١ - تحديد المسئوليات والسلطات درءاً لشيوع المسئولية والالتزام بالنظام من الكبير والصغير .

٢ - حصـول كـل مسـتخدم لنظام المعلومات والاتصالات علي مفتاح الدخول خاص به المختلف عن مفاتيح الغير للدخول إلي النظام .

٣ - أن يكون مفتاح الدخول مكون من ستة رموز علي الأقل .

٤ - وجوب تغير مفتاح الدخول بشكل متكرر وعشوائي .

٥ - وجـوب تغير مفتاح الدخول في حالة الاشتباه في معرفة غير المرخص له بمضمون المفتاح .

٦ - عدم احتواء مفتاح الدخول علي أي من الحروف الأولي لاسم المستخدم أو اختصار اسمه أو اسم شهر أو تاريخ ميلاد .

٧ - تكوين مفتاح الدخول بشكل عشوائي لتحقق من عدم احتوائه علي تسلسل رقمي أو منطقي .

٨ - إيجـاد الوسـائل الفنـية الآلية لتسجيل محاولات الاختراق الفاشلة للنظام وتسـجيل مـيعاد وتـاريخ حدوثها وكذلك تحديد الوحدة الطرفية التي تمت من خلالها محاولة الاختراق .

٩ - مناقشة وتحليل كل محاولات الاختراق غير الناجحة واتخاذ ما يلزم لتحصين النظام .

١٠ - تشفير وترميز المعلومات والبيانات الحساسة .

١١ - تغير مفاتيح التشفير بشكل متكرر غير دوري .

١٢ - إسناد مهمة إدارة مفاتيح التشفير لشخصين وليس لشخص واحد باستخدام نظام ثنائي منعاً من انفراد شخص بذلك .

١٣ - فصل خطوط الاتصالات غير اللازمة للدخول إلي نظم الحاسبات والمعلومات .

١٤ - قصر توزيع المعلومات والبيانات المشفرة والحساسة علي عدد محدود ومعلوم ومرخص له في تداول تلك البيانات بقدر ما يلزم .

١٥ - حصر توزيع المعلومات علي الأفراد أو الأقسام التي تكون تلك المعلومات لازمة وضرورية لها للقيام بوظائف تلك الأقسام أو الأعمال دون غيرها .

١٦ - الحفاظ علي البيانات في بنك بيانات محدد تتوافر له الحماية .

١٧ - تحديد مستويات الدخول إلي النظم بشكل متعدد الطبقات .

١٨ - متابعة اتصالات الموظفين خارج المنشأة وكذلك تنقلاتهم وحركاتهم بين الأقسام المختلفة علي أن يكون دخول الأقسام التي تحتوي علي معلومات حساسة بترخيص كتابي خاص .

١٩ - في حالة استخدام المعاملات المالية المشفرة تحفظ أرقام بطاقات الاعتماد في بنوك بيانات مستقلة غير متصلة بالشبكات ويجب آلا يتضمن تداول البيانات بين الأقسام الرقم الكامل لكارت الائتمان بل آخر ٤ أرقام فقط .

ج - الوسائل والأدوات الفنية لتوفير أمن المعلومات والاتصالات ومنها علي سبيل المثال : -

١ - تطبيق نظم إدارة وآمن المعلومات والاتصالات.

٢ - استخدام خطوط تليفونات واتصالات مأمونه .

٣ - استخدام وحدات تليفونات مؤمنة STU

٤ - استخدام قناة اتصالات آمنة.

٥ - اســتخدام تكنولوجيا الفخ الإيجابي TRAPPING POSITIVE وهو فلــتر يقــوم بتصيد التداخل في القنوات ويرفض ولوج غير المشتركين إلي تلك القناة.

٦ - اســتخدام تكنولوجيا الفخ السلبي TRAPPING NEGATIVE ويتم عــن طريقها حجز جزء من الإشارة وبالتالي منع حصول غير المشتركين علي الإشارة.

٧ - استخدام تكنولوجيا التشفير والترميز.

٨ - اســتخدام تكنولوجــيا SSL وهــي تكنولوجــيا تتضمن بروتوكولاً امنياً للإنترنت فيكون الولوج إلي النظام لمن هم مرخص لهم بذلك.

٩ - اســتخدام تكنولوجــيا التوقــيع الرقمــي أو الإلكتروني في مهر الرسائل الإلكترونية للتحقق من نسب المستند الإلكتروني لمنشئه ومرسله.

١٠ - اســتخدام خدمات التحقق والتصديق الإلكتروني وهي خدمات متاحة عن طــريق سلطات كهيئات البريد في بعض الدول أو بعض الشركات المرخص لها وهــي توفر تحققاً للمتعامل في التجارة الإلكترونية من شخصية مرسل البيانات أو الطرف الآخر في العلاقات التعاقدية الإلكترونية.

١١ - استخدام وسائل التأكد من صحة وسلامة المراسلات الإلكترونية .

١٢ - استخدام البرامج المضادة للفيروسات وتحديثها بانتظام.

١٣ - استخدام تكنولوجيا الحوائط النارية لحماية نظم الحاسبات والمعلومات.

١٤ - استخدام تكنولوجيا الــ TUNNCLING لتوفر نقل مؤمن للاتصالات

عبر الإنترنت أو غيره من الشبكات.

١٥ - استخدام تكنولوجيا الكشف عن وسائل التنصت في النظم والشبكات.

١٦ - استخدام الـ COOKIES FILE لإزاحة تلك الوسائل التي تستخدم في الدخول غير المشروع للنظام للتلصص عليه .

١٧ - اســتخدام تكنولوجيا العلامات المائية أو الأختام الإلكترونية الخاصة علي الوثائق الإلكترونية.

١٨ - استخدام الوسائط التكنولوجية الجديدة للدخول إلي النظم ومن ذلك ماسح بصمة اليد أو قزحية أو شبكة العين.

١٩ - استخدام تكنولوجيا الإجابة والتأكيد أو تكرار التأكيد.

٢٠ - استخدام تكنولوجيا تسجيل حدوث الاتصالات.

٢١ - اللجوء لخدمات شخص ثالث مؤمن لإيداع الوثائق الإلكترونية.

٢٢ - اســتخدام الـنقود الإلكترونــية فــي المعاملات الإلكترونية درءاً للنصب والاحتيال والسرقة.

و أخيرا لابد من تتبلور أي محاولة من المحاولات التي تبذل سواء من مصر أو مــن أي دولة أو منظمة أخري لابد من تتبلور تلك المحاولة في أطار عام يتركز حول أمن المعلومات على شبكة الإنترنت : -

أمن المعلومات عبر شبكة الإنترنت

INFORMATION SECURITY TRANS THE INTERNET

للعمــل على تحقيق أمن للكم الهائل من المعلومات الموجود على شبكة الإنترنت لابد من اتخاذ العديد من الخطوات إلا انه يمكن تقسيم تلك الخطوات إلى ثلاثة

اتجاهات هي : -

١ - سرية المعلومات

SECRECY OF INFORMATION

أي ضمان حفظ المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عـبر شـبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا في عدم إمكانـية الاطـلاع علـى تلك المعلومات إلا لمن هم مخول إليهم قانونا الاطلاع عليها فقط دون أن يتمكن أي من الغير من الاطلاع على تلك المعلومات ٠

٢ - سلامة المعلومات

SAFETY OF INFORMATION

أي ضـمان عـدم تغيير تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا في عدم إمكانية تغيير تلك المعلومات إلا لمن هم مخول قانونا إليهم تغييرها فقط دون أن يتمكن أي من الغير من تغيير تلك المعلومات ٠

٣ - وجود المعلومات

REFINDING OF INFORMATION

أي ضـمان عـدم حذف تلك المعلومات المخزنة على أجهزة الحاسبات الآلية أو تلك المنقولة عبر شبكة الإنترنت و الخطوات التي يجب اتخاذها هنا تصب جميعا فـي عدم إمكانية حذف تلك المعلومات إلا لمن هم مخول قانونا إليهم حذفها فقط دون أن يتمكن أي من الغير من حذف تلك المعلومات ٠

الـــفـــهـــرس

كتب سابقة المؤلفان

١ - الصيغ القانونية لعقود تأسيس الشركات

٢ - العلامات و البيانات و الأسماء التجارية

٣ - العقود التجارية

٤ - أعمال البنوك

٥ - الصيغ القانونية لدعاوى الشركات

٦ - الدفوع التجارية

٧ - عقد نقل التكنولوجيا

٨ - التوقيع الإلكتروني

مراجع الكتاب

- داود حسن طاهر - جرائم نظم المعلومات - الرياض - أكاديمية نايف العربية للعلوم الأمنية

- عز الدين احمد جلال - أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الإرهاب - الرياض - أكاديمية نايف العربية للعلوم الجنائية

- موقع الأستاذ / المنشاوى - على الإنترنت
WWW.MINSHAWI.COM

- موقع مجلس التعاون الخليجي
WWW.GCCSG.ORG

- موقع صحيفة ألبي بي سي
WWW.BBC.CO.UK

- محمد عادل ريان - جرائم الحاسب الآلي و امن البيانات - العربي (٤٤٠) ٧٣ - ٧٧

- مؤلفنا - التوقيع الإلكتروني و حجيته في الإثبات

- الجرائم المتعلقة باستخدام البطاقات الممغنطة / الدكتور - على عبد القادر القهوجي

- قرار الجمعية العامة للأمم المتحدة رقم ٥١ / ١٦٢ في ١٦ / ١٢ / ١٩٩٦

- إصدارات الأمم المتحدة - الجمعية العامة - لجنة الأمم المتحدة للقانون التجاري الدولي - الدورة الثالثة و الثلاثون - نيويورك - ٥ / ٤ / ٢٠٠٠)


Bibliotheca Alexandrina
0916960